

Contents

Introduction 1

| | |
|---|----|
| Product Description | 1 |
| Access Procedures. | 3 |
| How to Recover From a Lost Password | 6 |
| Upgrading Firmware through a Serial Connection. | 8 |
| Front Panel | 10 |
| Watchdog Features | 14 |

Control Console 15

| | |
|---------------------------------|----|
| How to Log On | 15 |
| Main Screen. | 18 |
| Control Console Menus | 21 |

Web Interface 24

| | |
|---------------------------|----|
| How to Log On | 24 |
| Summary Page | 27 |
| Navigation Menu | 29 |

Device and Outlet Management Menus 33

| | |
|--|----|
| How to Configure and Control Outlet Groups. | 33 |
| Outlet Settings for Outlets and Outlet Groups | 42 |
| Switched Rack PDU Settings. | 46 |
| Scheduling Outlet Actions (Web Interface Only) | 49 |

Event-Related Menus 53

| | |
|--|----|
| Introduction. | 53 |
| Event Log | 55 |
| Event Actions (Web Interface Only). | 60 |
| Event Recipients. | 63 |
| E-mail Feature | 64 |
| How to Configure Individual Events | 68 |

Data Menu (Web Interface Only) 69

Log Option 69
Configuration Option 70

Network Menu 71

Introduction 71
Option Settings 73

System Menu 96

Introduction 96
Option Settings 98

Boot Mode 110

Introduction 110
DHCP Configuration Settings 112

Security 117

Security Features 117
Encryption 122
Creating and Installing Digital Certificates 126
Firewalls 133

Using the APC Security Wizard 134

Overview 134
Create a Root Certificate & Server Certificates 137
Create a Server Certificate and Signing Request 142
Create an SSH Host Key 146

APC Device IP Configuration Wizard 148

Purpose and Requirements 148
Install the Wizard 149
Use the Wizard 150

How to Export Configuration Settings 153

Retrieving and Exporting the .ini File 153
The Upload Event and Error Messages 158
Using the APC Device IP Configuration Wizard. 160

File Transfers 161

Introduction 161
Upgrading Firmware: Methods and Tools 162
Verifying Upgrades and Updates 170

Product Information 171

Warranty and Service 171
Life-Support Policy 173

Index 174

Introduction

Product Description

Features of the Switched Rack PDU

The APC® Switched Rack Power Distribution Unit (PDU) is a stand-alone, network-manageable device that provides current monitoring and allows programmable control of eight, sixteen, or twenty-four power outlets (depending on the model).

You can manage a Switched Rack PDU through its Web interface, its control console, the InfraStruXure® Manager, or SNMP:

- The Web interface supports using HTTPS access with Secure Sockets Layer (SSL) and using HTTP access.
- You can access the control console through a serial connection, Telnet, or Secure SHell (SSH).
- Your Rack PDU is compatible with the APC InfraStruXure system and can be monitored and managed through the InfraStruXure Manager.
- You can use an SNMP browser and the APC PowerNet® Management Information Base (MIB) to manage your Rack PDU.

Switched Rack PDUs have these additional features:

- Current monitoring per phase or bank
- Configurable alarm thresholds that provide network and visual alarms to help avoid overloaded circuits
- Independent outlet control
- Configurable power delays
- 24 independent outlet user accounts

- Four levels of user access accounts—Administrator, Device Manager, Read Only User, and Outlet User
- Event and data logging—the event log is accessible by Telnet, Secure CoPy (SCP), File Transfer Protocol (FTP), serial connection, or Web browser (using HTTPS access with SSL, or using HTTP access). The data log is accessible by Web Browser, SCP, and FTP
- E-mail notifications for Rack PDU and system events
- SNMP traps, Syslog messages, and e-mail notifications based on the severity level of Rack PDU and system events
- A selection of security protocols for authentication and encryption



Note

The Rack PDU does not provide power protection. Therefore, APC does not recommend plugging a unit directly into any unprotected power source, such as a wall outlet.

Initial setup

You must define the following three TCP/IP settings for the Switched Rack PDU before it can operate on the network:

- IP address of the Rack PDU
- Subnet mask
- IP address of the default gateway



See also

To configure the TCP/IP settings, see the *Installation and Quick Start* manual provided as a PDF file on the *Utility* CD that came with your Rack PDU and as a printed manual.

Access Procedures

Overview

The Switched Rack PDU has two internal interfaces (control console and Web interface) that allow you to manage the Rack PDU.



For more information about the internal user interfaces, see [Control Console](#) and [Web Interface](#).

The SNMP interface also allows you to use an SNMP browser with the PowerNet[®] Management Information Base (MIB) to manage the Rack PDU.



See also

To use the PowerNet MIB with an SNMP browser, see the *PowerNet[®] SNMP Management Information Base (MIB) Reference Guide* (\doc\en\mibguide.pdf), which is provided on the *Utility CD* that came with your Switched Rack PDU.

Access priority for logging on

Only one user at a time can log on to the Rack PDU to use its internal user interface features. The priority for access is as follows:

- Local access to the control console from a computer with a direct serial connection to the Rack PDU always has the highest priority.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer has priority over Web access.
- Web access, either directly or through the InfraStruXure Manager, has the lowest priority.

Types of user accounts

The Rack PDU has four levels of access (Administrator, Device Manager, Read-Only User, and Outlet User), all of which are protected by password and user name requirements.

- An Administrator can use all of the management menus available in the control console and the Web interface. The Administrator's default user name and password are both **apc**.
- A Device Manager can use only the following menus:
 - The **Device Manager** menu and its sub-menus in the control console, and all menus in the top section of the navigation panel of the Web Interface (**Switched Rack PDU** and **Outlets**).
 - The **Log** option in the **Events** menu in the Web interface. A Device Manager can also access the event log in the control console by pressing CTRL-L.

The Device Manager's default user name is **device**; the password is **apc**.

- An Outlet User can access only the following menus:
 - the **Control** option of the **Outlets** menu of the Web interface.
 - the **Device Manager** menu and the **Phase/Bank Monitor**, **Outlet Control**, and **Power Supply Status** sub-menus in the control console.
- A Read-Only User has the following restricted access:
 - Access through the Web interface only.
 - Access to the same menus as a Device Manager, but without the capability to change configurations, control devices, or delete data. Links to configuration options are visible but are disabled, and the event and data logs display no **Delete** button.

The Read-Only User's default user name is **readonly**, and the default password is **apc**.



To set **User Name** and **Password** values for the four account types, see [User Manager](#) and [Outlet User Manager](#).



Note

You must use the Web interface to configure values for the Read-Only User, and you must use the control console to configure values for an Outlet User.

How to Recover From a Lost Password

You can use a local computer, a computer that connects to the Rack PDU or other device through the serial port to access the control console.

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the serial cable (990-0144) to the selected port on the computer and to the configuration port at the Rack PDU:
3. Run a terminal program (such as HyperTerminal[®]) and configure the selected port as follows:
 - 9600 bps
 - 8 data bits
 - no parity
 - 1 stop bit
 - no flow control
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
 - The serial port is not in use by another application.
 - The terminal settings are correct as specified in step 3.
 - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER as many times as necessary to redisplay the **User Name** prompt, then use the default, **apc**, for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)

7. From the **Control Console** menu, select **System**, then **User Manager**.
8. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**.
9. Press CTRL-C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Upgrading Firmware through a Serial Connection



For a complete description of how to download a firmware upgrade for your Rack PDU, see [Upgrading Firmware: Methods and Tools](#). That section also explains how to use network-based file transfer tools, which complete a firmware upgrade more quickly than the XMODEM protocol described here, which uses a serial connection.

You can use a local computer that connects to the Rack PDU through the serial port on the front panel of the unit.

1. Select a serial port at the local computer, and disable any service which uses that port.
2. Use the supplied serial cable (940-0144) to connect the selected port to the serial port on the front panel of the Rack PDU.
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
5. Enter your user name and password (both **apc**, by default, for administrators only) and press the ENTER key.
6. From the **Control Console** menu, select, in order, **System, Tools, File Transfer**, and **XMODEM**.
7. At the prompt `Perform transfer with XMODEM-CRC?` type **YES**, and press ENTER.
8. The system will then prompt you to choose a transfer rate and to change your terminal settings to match the transfer rate. Press ENTER to set the Switched Rack PDU to accept the download.

9. In the terminal program, send the file using the XMODEM protocol. When the transfer finishes, the console will prompt you to restore the baud rate to normal.



Caution

Do not interrupt the download.

The Rack PDU will restart when the download is complete.

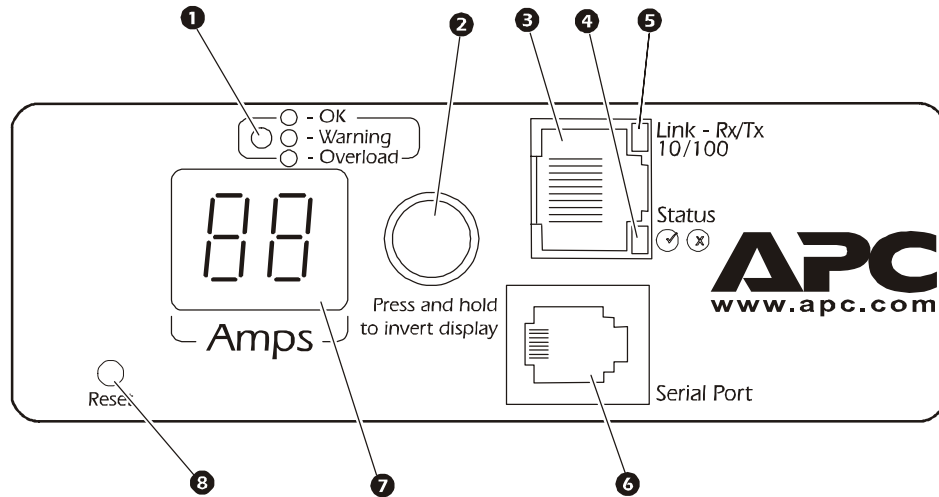


Note

Upgrading the firmware will not interfere with the operation of the outlets.

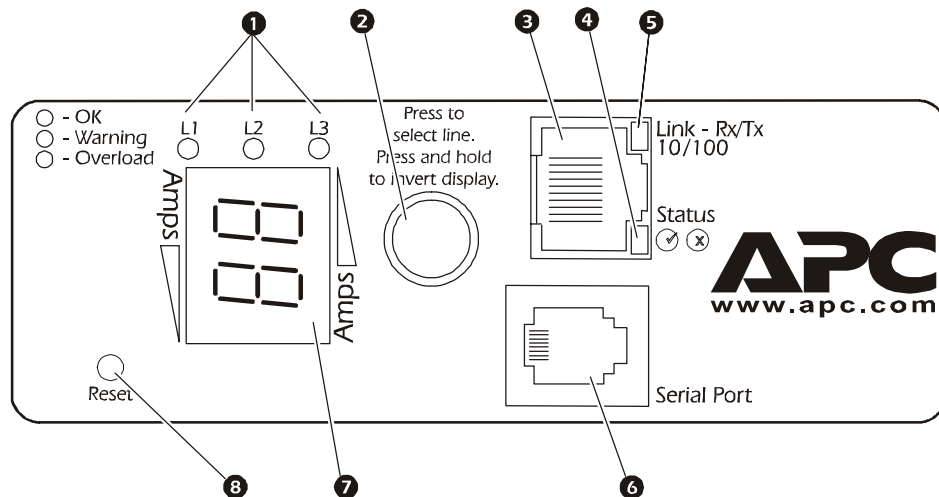
Front Panel

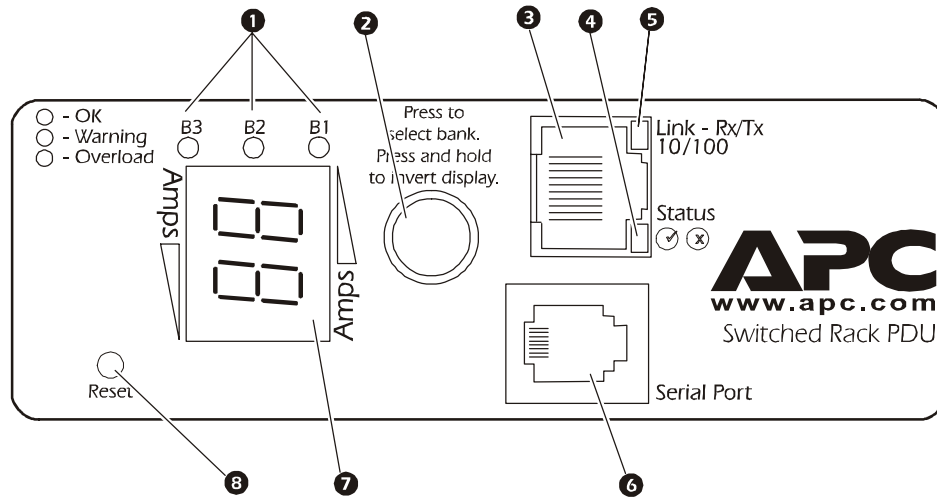
Single-phase



Three-phase

Three-phase Switched Rack PDUs have one of the following two front panels:





| Item | Function |
|---------------------------|---|
| ❶ Load Indicator LED | Identifies overload and warning conditions for the displayed phase or bank. See Load indicator LED . |
| ❷ Input Selector | On 3-phase models, press the input selector to monitor the current of the next phase or bank. For either 1- or 3-phase units, press and hold the input selector to display the IP address of the Rack PDU or to invert the display. At five seconds, the IP address is displayed; at ten seconds the displayed numbers invert. |
| ❸ 10/100 Base-T Connector | Connects the Rack PDU to the network. |
| ❹ Status LED | See Status LED . |
| ❺ Link-RX/TX LED | See Link-RX/TX (10/100) LED . |
| ❻ RJ-12 Serial Port | Connects the Rack PDU to a terminal emulator program for local access to the control console. (Use the supplied serial cable 940-0144.) |

| Item | Function |
|-------------------|---|
| 7 Digital Display | <p>Displays the current (amps) for the phase or bank indicated by the illuminated Load Indicator LED. On 3-phase units, the Digital Display will cycle through the phases or banks, displaying the current for each for 3 seconds.</p> <p>If an internal communication failure or power supply failure occurs (for either a 1- or 3-phase model), the Digital Display displays Er, which you can clear by pressing the input selector.</p> |
| 8 Reset Button | Resets the Rack PDU without affecting the outlet status. |

Link-RX/TX (10/100) LED

This LED indicates the network status.

| Condition | Description |
|-----------------------|--|
| Off | The device that connects the Rack PDU to the network is off or not operating correctly. |
| Flashing Green | The Rack PDU is receiving data packets from the network at 10 Megabits per second (Mbps). |
| Flashing Orange | The Rack PDU is receiving data packets from the network at 100 Megabits per second (Mbps). |
| Solid Green or Orange | The Rack PDU is not receiving any network traffic. |

Status LED

This LED indicates the network status of the Rack PDU.

| Condition | Description |
|---|--|
| Off | The Rack PDU has no power. |
| Solid Green | The Rack PDU has valid TCP/IP settings. |
| Flashing Green | The Rack PDU does not have valid TCP/IP settings. [†] |
| Solid Orange | A hardware failure has been detected in the Rack PDU. Contact APC Worldwide Customer Support . |
| Flashing Orange | The Rack PDU is making BOOTP requests. |
| Flashing Orange and Green (alternating) | The Rack PDU is making DHCP requests. |
| [†] If you do not use a BOOTP or DHCP server, see the <i>Installation and Quick Start</i> manual provided in PDF on the <i>Utility</i> CD that came with your Rack PDU and as a printed manual to configure the TCP/IP settings. | |

Load indicator LED

The load indicator LED identifies overload and warning conditions for the displayed phase or bank.

| Condition | Description |
|-------------|---|
| Solid Green | The current of the displayed phase or bank is below the Current Overload threshold. |
| Yellow | The displayed phase or bank is in a Near Overload Warning condition. The current is above the Near Overload Warning threshold. |
| Red | The displayed phase or bank is in an Overload condition. The current is above the Overload Alarm threshold. |

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Rack PDU uses internal, system-wide watchdog mechanisms. When it restarts itself to recover from an internal problem, a **System: Warmstart** event is recorded in the event log.

Network interface watchdog mechanism

The Rack PDU implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Rack PDU does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts itself.

Resetting the network timer

To ensure that the Rack PDU does not restart if the network is quiet for 9.5 minutes, the Rack PDU attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Rack PDU, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network most of the time and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the Rack PDU from restarting.

Control Console

How to Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection to access the control console.

Use case-sensitive **User Name** and **Password** entries to log on (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device Manager). A Read-Only User has no access to the control console.



If you cannot remember your user name or password, see [How to Recover From a Lost Password](#).

There is no default password for Outlet User accounts. (An Administrator must define the password and other account characteristics for an Outlet User.)



See [Outlet User Manager](#).

Remote access to the control console

You can access the control console through Telnet or Secure SHell (SSH), depending on which is enabled. (An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu.) By default, Telnet is enabled. Enabling SSH automatically disables Telnet.

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption. To use Telnet to access the control console from any computer on the same subnet:

1. At a command prompt, type `telnet` and the System IP address for the Rack PDU (when the PDU uses the default Telnet port of 23), and then press ENTER. For example:

```
telnet 139.225.6.133
```



Note

If the PDU uses a non-default port number (between 5000 and 32768), you need to include a colon or a space (depending on your Telnet client) after the IP address and then enter the port number.

2. Enter the user name and password (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device Manager).

SSH for high-security access. If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the control console. SSH encrypts user names, passwords and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Local access to the control console

You can use a local computer that connects to the Rack PDU through the serial port on the front panel of the unit.

1. Select a serial port at the local computer, and disable any service which uses that port.
2. Use the supplied serial cable (940-0144) to connect the selected port to the serial port on the front panel of the Rack PDU.
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.

Main Screen

Example main screen

The main screen that is displayed when you log on to the control console of a Rack PDU:

```
User Name : apc
Password  : ***

American Power Conversion          Network Management Card AOS   v2.6.4
(c) Copyright 2002 All Rights Reserved Rack PDU APP                 v2.6.6
-----
Name      : MS3 Test Unit                      Date : 6/25/2004
Contact   : Bill Cooper                        Time : 10:16:58
Location  : Testing Lab                        User  : Administrator
Up Time   : 0 Days 0 Hours 43 Minutes          Stat  : P+ N+ A+

Switched Rack PDU: Communication Established

----- Control Console -----

    1- Device Manager
    2- Network
    3- System
    4- Logout

<ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log
```

Information and status fields

Main screen information fields.

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware uses a name that identifies the type of device that connects to the network. In the [Example main screen](#), the application firmware for the Rack PDU is displayed.

```
Network Management Card AOS    v2.6.4
Rack PDU APP                    v2.6.6
```

- Three fields identify the system **Name**, **Contact**, and **Location** values.

```
Name       : MS3 Test Unit
Contact    : Bill Cooper
Location   : Testing Lab
```



To set the **Name**, **Contact**, and **Location** values, see [System Menu](#).

- An **Up Time** field reports how long the Rack PDU has been running since it was last reset or since power was applied.

```
Up Time    : 0 Days 0 Hours 43 Minutes
```

- Two fields identify when you logged on, by **Date** and **Time**.

```
Date : 6/25/2004
Time : 10:16:58
```

- A **User** field identifies whether you logged on as Administrator, Device Manager, or Outlet User.

```
User : Administrator
```

Main screen status fields.

- A **Stat** field reports the Rack PDU status.

Stat : P+ N+ A+

| | |
|----|---|
| P+ | The APC operating system (AOS) is functioning properly. |
| N+ | The network is functioning properly. |
| N? | A BOOTP request cycle is in progress. |
| N- | The Rack PDU failed to connect to the network. |
| N! | Another device is using the IP address of the Rack PDU. |
| A+ | The application is functioning properly. |
| A- | The application has a bad checksum. |
| A? | The application is initializing. |
| A! | The application is not compatible with the AOS. |



Note

If the AOS status is not P+, contact [APC Worldwide Customer Support](#), even if you can still access the Rack PDU.

- A Rack PDU model and name field reports the status of the Rack PDU. For example:

Switched Rack PDU: Communication Established

Control Console Menus

Menu structure

The menus in the control console list options by number and name. To use an option, type the corresponding number and press ENTER, then follow any on-screen instructions.

For menus that allow you to change a setting, you must use the **Accept Changes** option to save the changes you made.

While in a menu, you can also do the following:

- Type ? and press ENTER to access brief menu option descriptions (if the menu has help available).
- Press ENTER to refresh the menu.
- Press ESC to go back to the menu from which you accessed the current menu.
- Press CTRL-C to return to the main (control console) menu.
- Press CTRL-L to access the event log (Administrator and Device Manager only).



For information about the event log, see [Event-Related Menus](#).

Main menu

The main control console menu has options that provide access to the management features of the control console:

- 1- Device Manager
- 2- Network
- 3- System
- 4- Logout



Note

When you log on as Device Manager or as an Outlet User, you will not have access to the **Network** or **System** menus.

Device Manager option

This option accesses the **Device Manager** menu. Select the components you want to manage from this menu. To do any of the following tasks, see [Switched Rack PDU Settings](#):

- 1- Phase/Bank Monitor/Configuration
- 2- Phase/Bank Outlet Restriction Configuration
- 3- Outlet Control/Configuration
- 4- Power Supply Status

Option 4 is not available to outlet users.

Network option

To do any of the following tasks, see [Network Menu](#):

- Configure the TCP/IP settings for the Rack PDU or, when the Rack PDU will obtain its TCP/IP settings from a server, configure the settings for the type of server (DHCP or BOOTP) to be used.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet, Web interface and SSL, SNMP, e-mail, DNS, and Syslog features of the Rack PDU.

System option

To do any of the following tasks, see [System Menu](#):

- Control **Administrator**, **Device Manager**, and **Outlet User** access
- Define the system **Name**, **Contact**, and **Location** values
- Set the date and time used by the Rack PDU
- Restart the Rack PDU
- Reset control console settings to their default values
- Access system information about the Rack PDU

Web Interface

How to Log On

Overview

You can use the DNS name or System IP address of the Switched Rack PDU for the URL address of the Web interface.



Note

If you are using HTTPS (SSL/TSL) as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, when you log on you must use the same identifier for the Rack PDU as you specified for the common name in the certificate (either the IP address or the DNS name).

Use your case-sensitive user name and password settings to log on. The default user name differs by account type:

- **apc** for an Administrator
- **device** for a Device Manager
- **readonly** for a Read Only User

The default password is **apc** for all three account types.

There is no default password for Outlet User accounts. (An Administrator must define the password and other account characteristics for an Outlet User.)



See [Outlet User Manager](#).



See [Web/SSL \(Web/SSL/TLS in the control console\)](#) to select, enable, and disable the protocols that control access to the Web interface and to define the Web-server ports for the protocols.



For information about the Web page that appears when you log on to the Web interface, see [Summary Page](#).

Supported Web browsers

As your browser, you can use Microsoft[®] Internet Explorer (IE) 5.0 (and higher) or Netscape[®] 4.0.8 (and higher, except Netscape 6.x) to access the Rack PDU through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.

Data verification, the event log, and the data log require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

In addition, the Rack PDU cannot work with a proxy server. Therefore, before you can use a Web browser to access its Web interface, you must do one of the following:

- Configure the Web browser to disable the use of a proxy server for the Rack PDU.
- Configure the proxy server so that it does not proxy the specific IP address of the Rack PDU.

URL address formats

Type the Rack PDU's DNS name or IP address in the Web browser's URL address field and press ENTER. Except when you specify a non-default web server port in Internet Explorer, `http://` or `https://` is automatically added by the browser.



Note

If the error "You are not authorized to view this page" occurs (Internet Explorer only), someone is logged onto the Web interface or control console. If the error "No Response" (Netscape) or "This page cannot be displayed" (Internet Explorer) occurs, Web access may be disabled, or the Rack PDU may use a non-default Web-server port that you did not specify correctly in the address. (For Internet Explorer, you must type `http://` or `https://` as part of the address when any port other than 80 is used.)



For more information, see [Port assignments](#).

- For a DNS name of Web1, the entry would be one of the following:
 - `http://Web1` if HTTP is your access mode
 - `https://Web1` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Rack PDU uses the default port (80) at the Web server, the entry would be one of the following:
 - `http://139.225.6.133` if HTTP is your access mode
 - `https://139.225.6.133` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Rack PDU uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
 - `http://139.225.6.133:5000` if HTTP is your access mode
 - `https://139.225.6.133:5000` if HTTPS (SSL/TLS) is your access mode

Summary Page

When you log on to the Web interface at the Switched Rack PDU, the status view is at the right side of the screen, the quick status tab is at the upper right, and the navigation menu is at the left.





Status

The **Status** view has three sections:

- The **Device Status** section reports any active alarm or warning conditions and displays the load for each phase or bank, including a graphic representation of the load thresholds.
- The **Outlet Status** section shows the number, phase or bank (for 3-phase models), state (on, off), and name of the outlet.
- The **Switched Rack PDU Parameters** section shows the following:
 - The **Name**, **Contact**, and **Location** information for the Rack PDU
 - The date and time you logged on
 - The Type of User (**Administrator**, **Device Manager**, **Read Only User**, or **Outlet User**)
 - The time (**Up Time**) the Rack PDU has been running continuously since it was last reset or power was applied
 - The rating of the Rack PDU (1- or 3-phase, and the maximum number of amps per phase or bank)

Quick status tab

The quick status tab is displayed at the upper right on every page in the Web interface. The tab shows active alarms and warnings and a link to the online help.

| | |
|--|---|
|  | Click the help icon to access the online help for the displayed page. |
|  | Click the green “device operating normally” icon to return to the status screen where the current for each phase or bank is displayed. |
|  | Click the warning icon to return to the status screen where active warnings are displayed. Put the mouse cursor on the icon to view details of the warning. |
|  | Click the alarm icon to return to the status screen where active alarms are displayed. Put the mouse cursor on the icon to display details of the alarm. |

Navigation Menu

Overview

On the Web interface, the navigation menu (left frame) has the following elements:

- IP address of the Rack PDU
- Menus to manage the Rack PDU and its components:
 - **Switched Rack PDU** menu with **Configuration** and **Scheduling** as options
 - **Outlets** menu with **Control**, **Configuration**, and **Outlet Groups** as options
- Menus to manage the event log, data log, network connection, and system parameters:
 - **Events** menu
 - **Data** menu
 - **Network** menu
 - **System** menu



Note

When you log on as a Device Manager or Read-Only User, the **Network** and **System** menus are not displayed. Options to make any changes are not available for the Read-Only User.

When you log on as an Outlet User, the **Switched Rack PDU**, **Events**, **Network**, and **System** menus are not displayed.

- **Logout** option
- **Help** menu
- **Links** menu

Selecting a menu to perform a task

- To do the following, see [Switched Rack PDU Settings](#):
 - Configure the overload and low load thresholds for each phase or bank.
 - Configure the **Overload Outlet Restriction** for each phase or bank.
 - Set the **Name**, **Location**, and **Coldstart Delay** for the Rack PDU.
- To do the following, see [Outlet Settings for Outlets and Outlet Groups](#):
 - Apply power to and remove power from the outlets.
 - Set **Power On Delay**, **Power Off Delay**, and **Reboot Duration** for the outlets.
 - Set the names and associated links for the outlets.
 - Create, enable, and use synchronized outlet groups.
- To do the following, see [Event-Related Menus](#):
 - Access the event log.
 - Configure the actions to be taken based on the severity level of an event.
 - Configure **SNMP Trap Receiver** settings for sending event-based traps.
 - Define who will receive e-mail notifications and Syslog messages for events.
 - Test e-mail settings.
- To do the following, see [Data Menu \(Web Interface Only\)](#):
 - Access the data log.
 - Define the log interval (how often data will be sampled and recorded) for the data log.

- To do the following, see [Network Menu](#):
 - Configure new TCP/IP settings for the Rack PDU.
 - Identify the Domain Name System (DNS) Server, test its network connection, and enable or disable DNS Reverse Lookup Event Logging (which logs the domain name of the device associated with each event).
 - Define settings for FTP, Telnet, SSH, the Web interface, SNMP, e-mail, and SSL/TLS.
 - Configure the Rack PDU's Syslog message feature.
- To do the following, see [System Menu](#):
 - Control **Administrator** and **Device Manager** access.
 - Manage **Outlet User** access.
 - Define the system **Name**, **Contact**, and **Location** values.
 - Set the date and time used by the Rack PDU.
 - Restart the Rack PDU.
 - Reset control console settings to default settings.
 - Define the URL addresses of the user links and APC logo link in the Web interface, as described in [Links menu](#).

Help menu

When you click **Help**, the **Contents** page for all of the online help is displayed. However, from any Web interface pages, you can use the question mark (?) in the quick status bar to link to the section of the online help for that page.

The **About System** option of the **Help** menu displays information in the following fields: **Model Number**, **Serial Number**, **Hardware Revision**, **Manufacture Date**, **MAC Address**, **Application Module**, **APC OS (AOS) Module** (the APC Operating System Module of the Switched Rack PDU), and the date and time that each of the two modules were created.



Note

In the control console, the **About System** option, which is a **System** menu option, has the **Flash Type** value.

Links menu

Provides three user-definable URL link options. By default, these links access the following APC Web pages:

- **APC's Web Site** accesses the APC home page.
- **Testdrive Demo** accesses a demonstration page where you can use samples of APC Web-enabled products.
- **APC Monitoring** accesses the “APC Remote Monitoring Service” page about pay-for-monitoring services available from APC.

To redefine these links so that they point to other URLs:

1. Click on **Links** in the **System** menu.
2. Define any new names for **User Links**.
3. Define any new URL addresses that you want **User Links** to access. Only HTTP links may be defined.
4. Click **Apply**.



Note

The link associated with the APC logo is also definable.

Device and Outlet Management Menus

How to Configure and Control Outlet Groups

Outlet group terminology

An *outlet group* consists of outlets that are logically linked together on the same Switched Rack PDU. Outlets that are in an outlet group turn on, turn off, and reboot in a synchronized manner, i.e., within a one-second interval under normal conditions:

- A *local outlet group* consists of two or more outlets on a Switched Rack PDU. Only the outlets in that group are synchronized.
- A *global outlet group* consists of one or more outlets on a Switched Rack PDU. One outlet is configured as a *global outlet*, which logically links the outlet group to outlet groups on up to three other Switched Rack PDUs. All outlets in the linked global outlet groups are synchronized.
 - For global outlet groups, the *initiator outlet group* is the group that issued the action
 - For global outlet groups, a *follower outlet group* is any other outlet group that is synchronized with the initiator outlet group.

When you apply an outlet control action to outlets that are members of an outlet group, the outlets are synchronized as follows:

- For a global outlet group, use the delay periods and reboot duration configured for the global outlet of the initiator outlet group.
- For a local outlet group, the outlets use the delay periods and reboot duration of the lowest-numbered outlet in the group.

Purpose and benefits of outlet groups

By using groups of synchronized outlets on Switched Rack PDUs, you can ensure that outlets turn on, turn off, and reboot in a synchronized manner. Synchronizing control group actions through outlet groups provides the following benefits.

- Synchronized shutdown and startup of the power supplies of dual-corded servers avoids erroneous reporting of power supply failures during a planned system shutdown or reboot.
- Synchronizing outlets by using outlet groups provides more precise shutdown and restart timing than relying on the delay periods of individual outlets.
- A global outlet is visible to the user interfaces of the Switched Rack PDUs to which it is linked.



Note

Under normal conditions all outlets in outlet groups affected by a control action will perform that action within a one-second interval.

System requirements for outlet groups

To set up and use synchronized outlet control groups:

- You need a 10/100Base-T TCP/IP network, with an Ethernet hub or switch that has a power source not shared by the computers or other devices being synchronized.
- If outlets groups are to be synchronized across multiple Switched Rack PDUs, those Switched Rack PDUs must meet the following requirements:
 - They must be on the same subnet.
 - They must use firmware that has the same version number, which must be 2.6.1 or higher for both the APC Operating System (AOS) module and the Application module. As later firmware revisions become available, be sure to upgrade each Switched Rack PDU.
- You need a computer that can initiate synchronized control operations through the Web interface or control console of the Switched Rack PDUs or through SNMP.
- You must ensure that Multicast network traffic is allowed for the selected Multicast IP address by each switch that connects the Switched Rack PDUs.

Rules for configuring outlet groups

For a system that uses outlet groups, the following rules apply:

- A Switched Rack PDU can have more than one outlet group, but an outlet can belong to only one outlet group.
- A local outlet group, which has no global outlet, must consist of two or more outlets.
- You can synchronize a global outlet group on one Switched Rack PDU with a global outlet group on each of three other Switched Rack PDUs.
 - In a global outlet group, you can designate only one outlet to be a global outlet, linking to outlet groups on other Switched Rack PDUs for the purpose of synchronization. That global outlet can be the only outlet in its group, or the group can consist of multiple outlets.
 - For outlet groups on Switched Rack PDUs to be linked for synchronization, those Switched Rack PDUs must have the same Device Multicast Name and Device Multicast Address and be running the same version of Switched Rack PDU firmware.
 - A global outlet of one outlet group must have the same physical outlet number as the global outlet of any other outlet group to which it links.
 - Even if InfraStruXure Manager is not used with your system, you must enable the ISX Protocol for each Switched Rack PDU to link global outlet groups across Switched Rack PDUs.



To enable the ISX Protocol, see [ISX Protocol \(control console only\)](#).

- To create and configure outlet groups, you must use the Web interface or export configuration file (.ini file) settings from a configured Switched Rack PDU. The control console lets you display whether an outlet is a member of an outlet group and to apply control actions to an outlet group, but does not let you set up or configure an outlet group.

How to enable outlet groups

From the **Outlets** menu in the Web interface, select **Outlet Groups**, configure the following parameters, and click **Apply**.

Enable creation of outlet groups.

| Parameter | Description |
|---------------------------|---|
| Device Level Outlet Group | To create an outlet group, you must enable this parameter. It is disabled by default. |

Enable support for global outlet groups (linked groups).

| Parameter | Description |
|----------------|---|
| Multicast Name | To link outlet groups on multiple Switched Rack PDUs, you must define the same Multicast name and Multicast IP address on each of those Rack PDUs. NOTE: A Maximum of four devices can be configured with the same Multicast name and Multicast IP address. |
| Multicast IP | |

How to create a local outlet group (Web interface)

1. From the **Outlets** menu in the Web interface, select **Outlet Groups**.
2. Make sure outlet groups are enabled.



See [Enable creation of outlet groups](#).

3. Click **Create Local Outlet Group**.
4. Under **Configure Local Outlet Group**, select each outlet that will be in the group. You must select at least two outlets.

How to create multiple global outlet groups (Web interface)

To set up multiple global outlet groups that link to outlet groups on other Switched Rack PDUs:

1. From the **Outlets** menu in the Web interface, select **Outlet Groups**.
2. Make sure outlet groups are enabled and that the Multicast parameters (name and IP address) are the same for all Rack PDUs to be linked.



See [How to enable outlet groups](#).

3. Click **Create Global Outlet Groups**.
4. For each global outlet group you want to create, select an outlet by clicking on its check-box. Then click **Apply**. For example, select five outlets to create five outlet groups, each consisting of one global outlet.
5. To add outlets to any of the global outlet groups you created, see [How to edit or delete an outlet group](#).

How to edit or delete an outlet group

1. From the **Outlets** menu in the Web interface, select **Outlet Groups**.
2. Under **Configured Outlet Groups**, click on the number or name of the outlet group to edit or delete.
3. When editing an outlet group you can do any of the following:
 - Rename the outlet group.
 - Add or remove outlets by clicking the check-boxes to mark or unmark them.



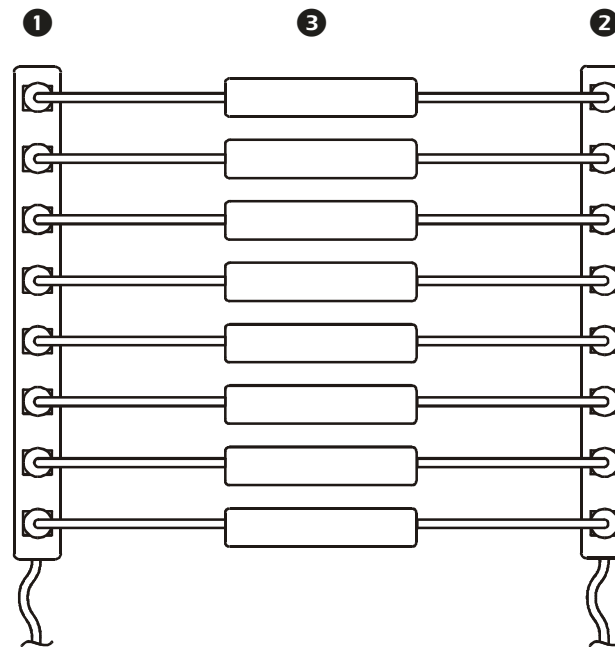
Note

You cannot remove an outlet from an outlet group that contains only two outlets unless the remaining outlet is a global outlet.

4. To delete the outlet group, click **Delete Outlet Group**.

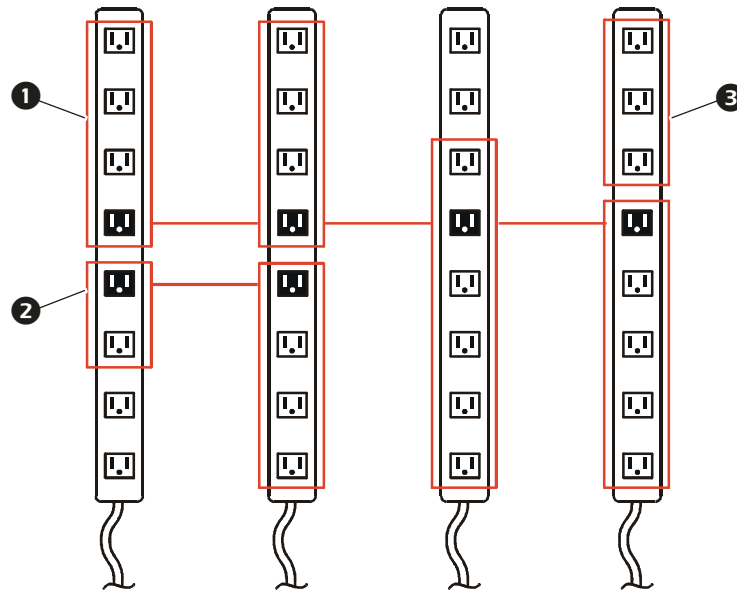
Typical outlet group configurations

The following configuration shows two Switched Rack PDUs, each with eight outlet groups. Each outlet group consists of a single global outlet. Each outlet group ❶ on the first Switched Rack PDU is linked to the outlet group ❷ in the same location on the second Switched Rack PDU. One power cord of a dual-corded server ❸ is connected to each outlet on the first Switched Rack PDU, and its other cord is connected to the corresponding outlet on the second Switched Rack PDU, ensuring that output power from both power sources to the server will turn on or off in a synchronized manner in response to an outlet control action.



The following configuration shows three sets of synchronized outlets. Global outlets are shown in black. Outlet groups are enclosed in red rectangles.

| | |
|----------|--|
| 1 | These four global outlet groups synchronize a total of 19 outlets. |
| 2 | These two global outlet groups synchronize 6 outlets, 2 in one group and 4 in the other. |
| 3 | This local outlet group synchronizes 3 outlets on the same Switched Rack PDU. |



Verify your setup and configuration for global outlet groups

To ensure that your setup meets all system requirements for outlet group and that you have configured the outlet groups correctly, select **Outlet Groups** from the **Outlets** menu in the Web interface to view the groups and their connections:

- The **Configured Outlet Groups** section displays the following:
 - All configured outlet groups on the current Switched Rack PDU.
 - The outlets in each group by outlet number.
 - Any outlet groups on other Switched Rack PDUs with which a global outlet group is synchronized. Each Switched Rack PDU is identified by its IP address, and each global outlet is displayed in bold text.
- The **Global Outlet Overview** section displays the following:
 - The IP address of the current Switched Rack PDU.
 - The IP address of any Switched Rack PDUs that contain global outlets that are available to be synchronized with outlet groups on other Switched Rack PDUs.
 - All global outlets configured on the Switched Rack PDUs listed, regardless of whether they are synchronized with outlet groups on the current Switched Rack PDU.

Outlet Settings for Outlets and Outlet Groups

How to initiate a control action



Note

If you apply an outlet control action to outlets or outlet groups, the following delays are used for the action:

- For an individual outlet (not in an outlet group), the action uses the delay periods and reboot duration configured for that outlet.
- For a global outlet group, the action uses the delay periods and reboot duration configured for the global outlet.
- For a local outlet group, the action uses the delay periods configured for the lowest-numbered outlet in the group.

Web interface. To control the outlets on your Switched Rack PDU

1. Select **Outlets**, and then **Control** on the navigation menu.
2. Mark the check-boxes for each individual outlet or outlet group to control, or select the **All Outlets** check-box.
3. Select a **Control Action** from the list, and click **Next >>**. On the confirmation page that explains the action, choose to execute or cancel it.

Control Console. Select **Outlet Control/Configuration** from the **Device Manager** menu to display a list of outlets. For each outlet, the list indicates whether it is a member of an outlet group.

1. Choose either or the following:
 - To control one outlet and the outlet group, if any, to which it belongs, select the number of the outlet, and then select **Control Outlet**.
 - To control all outlets, select **Master Control/Configuration**, and then **Control of ALL Outlets**.
2. Select a control action.
3. On the confirmation screen that describes the action to be executed, type `Yes` at the prompt to perform the action.

Control actions you can select.

| Option | Description |
|--|--|
| No Action (Web interface only) | Do nothing. |
| On Immediate | Apply power to the selected outlets. |
| On Delayed | Apply power to each selected outlet according to its value for Power On Delay .† |
| Off Immediate | Remove power from the selected outlets. |
| Off Delayed | Remove power from each selected outlet according to its value for Power Off Delay .† |
| Reboot Immediate | Remove power from each selected outlet. Then apply power to each of these outlets according to its value for Reboot Duration .† |
| Reboot Delayed | Remove power from each selected outlet according to its value for Power Off Delay . Wait until all outlets are off (the highest value for Reboot Duration), and then apply power to each outlet according to its value for Power On Delay .† |
| Cancel Pending Commands (Web Interface) Cancel (control console) | Cancel all commands pending for the selected outlets and keep them in their present state. NOTE: For global outlet groups, you can cancel a command only from the interface of the initiator outlet group. The action will cancel the command for the initiator outlet group and all follower outlet groups. |
| † If a local outlet group is selected, only the configured delays and reboot duration of the lowest-numbered outlet of the group are used. If a global outlet group is selected, only the configured delays and reboot duration of the global outlet are used. | |

How to configure outlet settings and outlet name

Settings that you can configure. The following settings are available in both the Web interface and control console unless otherwise indicated:

| Setting | Description |
|---|---|
| Power On Delay | <p>Set the number of seconds that the Rack PDU waits after a command is issued before applying power to an outlet.</p> <p>NOTE: To configure an outlet to remain off at all times, check the Never check box next to Power On Delay in the Web interface, or configure a value of -1 for Power On Delay in the control console.</p> |
| Power Off Delay | <p>Set the number of seconds that the Rack PDU waits after a command is issued before removing power from an outlet.</p> <p>NOTE: To configure an outlet to remain on at all times, check the Never check box next to Power Off Delay in the Web interface, or configure a value of -1 for Power Off Delay in the control console.</p> |
| Reboot Duration | <p>Set the number of seconds an outlet remains off before restarting.</p> |
| Name (Web interface) Outlet Name (control console) | <p>Set the name for one or more outlets. The name is displayed next to the outlet number on status screens.</p> |
| Link (Web interface) | <p>Define an HTTP or HTTPS link to a Web site or IP address.</p> <ul style="list-style-type: none">• http://www.apcc.com links the outlet to the home page of the APC Web site.• http://158.205.7.201 links the outlet to the Web interface of the Switched Rack PDU at the IP address 158.205.7.201, enabling you to log on to that interface (if you have the appropriate access). <p>NOTE: If the outlet is a member of an outlet group, the only link that is used is the link configured for the global outlet or (for a local outlet group) the link configured for the lowest-numbered outlet of a local outlet group. You can configure a link for another outlet in an outlet group, but that link will be available to use only when that outlet is no longer a member of an outlet group.</p> |

Web Interface. To configure the outlet settings or outlet names, select **Configuration** on the **Outlets** menu, and click the **Configure** button in the **Outlet Settings** section or in the **Outlet Name Configuration** section.

- Configure outlet settings in the top section of the next screen:
 - Select the check-boxes next to the numbers of the outlets you want to modify, or select the **All Outlets** check-box.
 - Enter values for **Power On Delay**, **Power Off Delay**, or **Reboot Duration**, and click the **Apply** button immediately below the list.
- Configure outlet names and links in the bottom section of the next screen:
 - Select the check boxes next to the numbers of the outlets you want to modify, or select the **All Outlets** check-box.
 - Enter values for **Name** and **Link**, and click the **Apply** button immediately below the list.

Control Console. To configure the outlet settings and outlet name:

1. Select **Outlet Control/Configuration** from the **Device Manager** menu.
2. Choose the number of the outlet you want to control, and press ENTER.
3. Choose **Configure Outlet** to display and change the values for **Outlet Name**, **Power On Delay**, **Power Off Delay**, and **Reboot Duration**.

Switched Rack PDU Settings

Configure Load Thresholds

Web interface.

1. Select **Switched Rack PDU** from the navigation menu.
2. Click **Configure** in the **Load Management** section.
3. Set **Overload Alarm Threshold**, **Near Overload Warning Threshold**, **Low Load Warning Threshold**, and **Overload Outlet Restrictions** for each phase or bank.
4. Click **Apply** in that section to set the selected values.

Control console.

1. From the **Device Manager** menu, select **Phase/Bank Monitor/Configuration**.
2. Select a phase or bank (for 3-phase units).
3. Select **Overload Alarm Threshold (amps)**, **Near Overload Warning Threshold (amps)**, or **Low Load Warning Threshold (amps)**.
4. Select **Accept Changes**.

To set the overload outlet restriction, select **Outlet Restriction Configuration** on the **Device manager** menu. For 3-phase units, select a phase or bank to display and change the **Outlet Phase/Bank Restriction**.

| Setting | Description |
|---------------------------------|---|
| Overload Alarm Threshold | Set the number of amps that will cause an overload of this phase or bank. |
| Near Overload Warning Threshold | Set the number of amps at which to generate a warning that the Rack PDU is nearing overload of a phase or bank. |

| Setting | Description |
|-----------------------------|--|
| Low Load Warning Threshold | Set the low threshold, in amps, for the current drawn from this phase or bank during normal operation. A load at or below this level generates a warning. |
| Overload Outlet Restriction | Prevent users from applying power to outlets during an overload condition. You can set the following restrictions for each outlet: <ul style="list-style-type: none"> • None: You can apply power to outlets regardless of an Overload Alarm or Near Overload Warning. • On Warning: You cannot apply power to an outlet on the selected phase or bank if the current for that phase or bank has exceeded the Near Overload Warning threshold. • On Overload: You cannot apply power to an outlet on the selected phase or bank if the current for that phase or bank has exceeded the Overload Alarm threshold. |

How to configure Device Settings

Web interface. Select **Configuration** on the **Switched Rack PDU** menu. Then, under **Device Settings**, click the **Configure** button and configure the **Name** and **Location** fields for the Rack PDU, and set the **Coldstart Delay**.

Control console.

1. Select **Outlet Control/Configuration** from the **Device Manager** menu.
2. Select **Master Control/Configuration** from the displayed list.
3. Select **Master Outlet Configuration** from the next menu displayed.
4. Change the **Name**, **Location**, or **Coldstart Delay** from this menu.

| Setting | Description |
|-----------------|---|
| Name | Set the name of the Rack PDU. |
| Location | Set the location of the Rack PDU. |
| Coldstart Delay | The time that the Switched Rack PDU delays applying power to the outlets after AC power has been applied to the Rack PDU. |



To change the **Contact** field (the name of the person to contact about the Rack PDU) in addition to the **Name** and **Location** fields in the control console, see [Identification](#).

Power Supply Status (control console only)

Select **Power Supply Status** from the **Device Manager** menu to display the status of the power supplies of the Switched Rack PDU.

Scheduling Outlet Actions (Web Interface Only)

Actions you can schedule

For any outlets you select, you can schedule any of the following actions to occur daily; at intervals of one, two, four, or eight weeks; or only once.



To configure values for **Power On Delay**, **Power Off Delay**, and **Reboot Duration** for each outlet, see [How to configure outlet settings and outlet name](#). Although you must use the Web interface to schedule outlet actions, you can set these values in either the Web or control console interfaces.



Note

For an action to be applied to an outlet group, you must have outlet groups enabled at the beginning of the scheduled action. For example, if **Off Delayed** is scheduled for 4:00 p.m., the **Power Off Delay** begins at 4:00 p.m. Even if you then enable outlet groups during that **Power Off Delay** before any of the outlets are scheduled to turn off, the action will be applied only to the individual outlet and not the outlet group.

| Option | Description |
|---------------|---|
| No Action | Do nothing. |
| On Immediate | Apply power to the selected outlets. |
| On Delayed | Apply power to each selected outlet according to its value for Power On Delay . [†] |
| Off Immediate | Remove power from the selected outlets. |

[†] If an outlet group is selected, the configured delays and reboot duration of the lowest-numbered outlet (for a local outlet group) or of the global outlet (for a global outlet group that is initiating the action).

| Option | Description |
|--|--|
| Off Delayed | Remove power from each selected outlet according to its value for Power Off Delay . [†] |
| Reboot PDU Immediate | Remove power from each selected outlet. Then apply power to each of these outlets according to its value for Reboot Duration . [†] |
| Reboot PDU Delayed | Remove power from each selected outlet according to its value for Power Off Delay . Wait until all outlets are off (the highest value for Reboot Duration), and then apply power to each outlet according to its value for Power On Delay . [†] |
| <p>† If an outlet group is selected, the configured delays and reboot duration of the lowest-numbered outlet (for a local outlet group) or of the global outlet (for a global outlet group that is initiating the action).</p> | |

How to schedule an outlet event

1. From the menus of the Web interface, select **Switched Rack PDU** and then **Scheduling**.
2. On the **Outlet Scheduling** page, select how often the event will occur: **Daily**, **Weekly**, or **One-Time**.



Note

If you select **Weekly**, you can choose to have the event occur once every week or once every two, four, or eight weeks.

3. On the scheduling page, in the **Name of event** text box, replace the default name, `Outlet Event`, with a name that will identify your new event.
4. Use the drop-down lists to select the type of event and when it will occur.



Note

The date format for one-time events is *mm/dd*, and the time format for all events is *hh/mm*, with the two-digit hour specified in 24-hour time.

- An event that is scheduled daily or at one of the intervals available in the **Weekly** selection continues to occur at the scheduled interval until the event is deleted or disabled.
 - You can schedule a one-time event to occur only on a date within 12 months of the date on which you perform the scheduling. For example, on June 4, 2004, you could schedule a one-time event on any date from the current date until June 3, 2005.
5. Use the check-boxes to select which outlets will be affected by the action. You can select one or more individual outlets or **All Outlets**.
 6. Click **Apply** to confirm the scheduling of the event, or **Clear** to cancel it.

When you confirm the event, the summary page is re-displayed, with the new event displayed in the list of scheduled events.

How to edit, disable, enable, or delete an outlet event

1. From the menus of the Web interface, select **Switched Rack PDU** and then **Scheduling**.
2. In the event list in the **Summary** section of the **Outlet Scheduling** page, click on the name of the event.
3. On the **Scheduled Event Details** page, you can do any of the following:
 - Change details of the event, such as the name of the event, when it is scheduled to occur, and which outlets are affected.
 - Under **Status of event** at the bottom of the page:
 - Disable the event, leaving all its details configured so that it can be re-enabled later. A disabled event will not occur. An event is enabled by default when you create it.
 - Enable the event, if it was previously set to **Disable**.
 - Delete the event, removing the event completely from the system. A deleted event cannot be retrieved.
4. Click **Clear** at any time to cancel your changes to the event. Using **Clear** cancels only the changes you made in the current editing session.
5. When you finish making changes on this page, click **Apply** to confirm the changes.

Event-Related Menus

Introduction

Overview

The **Events** menu provides access to the options that you use to do the following tasks:

- Access the event log
- Define the actions to be taken when an event occurs, based on the severity level of that event:
 - Event logging
 - Syslog message notification
 - SNMP trap notification
 - E-mail notification



Note

You can use only the Web interface to define which events will use which actions, as described in [Event Log](#) and [How to Configure Individual Events](#).

- Define up to four SNMP trap receivers, by NMS-specific IP address or domain name, for event notifications by SNMP traps.
- Define up to four recipients for event notifications by e-mail.

Menu options

In the Web interface, all of the events options are accessed through the **Events** menu.

In the control console, access the available events-related options as follows:

- Use the **Email** option in the **Network** menu to define the SMTP server and e-mail recipients.
- Use the **SNMP** option in the **Network** menu to define the SNMP trap receivers.
- Use CTRL-L to access the event log from any menu.

For information on the following topics, use these links:

- [Event Log](#)
- [Event Actions \(Web Interface Only\)](#)
- [Event Recipients](#)
- [E-mail Feature](#)
- [How to Configure Individual Events](#)

Event Log

Overview

The Rack PDU supports event-logging for all embedded management card application firmware modules. To record and display embedded management card and Rack PDU events, use any of the following to view the event log:

- Web interface
- Control console
- FTP
- SCP

Logged events

By default, any event which causes an SNMP trap will be logged, except for SNMP authentication failures. Additionally, the Rack PDU will log its abnormal internal system events. However, you can use the **Actions** option in the Web interface's **Events** menu to disable the logging of events based on their assigned severity level, as described in [Event Actions \(Web Interface Only\)](#).



Note

Some System (embedded management card) events do not have a severity level. Even if you disable the event log for all severity levels, events with no severity level will still be logged.



To access a list of the System (embedded management card) and Switched Rack PDU (Device) events, see [Event List page](#).

Web interface

The **Log** option in the **Events** menu accesses the event log. This log displays all of the events that have been recorded since the log was last deleted, in reverse chronological order. The **Delete Log** button clears all events from the log.

Control console

Press CTRL-L to display all the events that have been recorded since the log was last deleted, in reverse chronological order. Use the SPACE BAR to scroll through the recorded events. While viewing the log, type d and press ENTER to clear all events from the log.



Note

After events are deleted, they cannot be retrieved.

How to use FTP or SCP to retrieve a log file



Note

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file. (You should have FTP disabled.) If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.



See [Security](#) for information on the available protocols and methods for setting up the type of security appropriate for your needs.

If you have Administrator or Device Manager access, you can use SCP or FTP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) that you can import into a spreadsheet application.

- The file reports all of the events or data recorded since the log was last deleted.
- The file includes information that the event log or data log does not display.
 - The version of the file format (first field)
 - The **Date** and **Time** the file was retrieved
 - The **Name**, **Contact**, and **Location** values, and the IP address of the Rack PDU
 - The unique **Event Code** for each recorded event (*event.txt* file only)



Note

The Rack PDU uses a 4-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits of the year.

Secure CoPy (SCP).

To use SCP to retrieve the *event.txt* file, use the following command:

```
scp username@hostname_or_ip_address:event.txt ./event.txt
```

To use SCP to retrieve the *data.txt* file, use the following command:

```
scp username@hostname_or_ip_address:data.txt ./data.txt
```



See [Data Menu \(Web Interface Only\)](#) for information about the data log.

File Transfer Protocol (FTP).

To use FTP to retrieve the *event.txt* or *data.txt* file:

1. At a command prompt, type `ftp` and the IP address of the Switched Rack PDU, and press ENTER. If the **Port** setting for **FTP Server** in the **Network** menu has been changed from its default value (21), you must use the non-default value in the FTP command. For some FTP clients, you must use a colon to add the port number to the end of the IP address. For Windows FTP clients, use the following command (including spaces):

```
ftp>open ip_address port_number
```



To use non-default port values to enhance security, see [Port assignments](#).

2. Use the case-sensitive **User Name** and **Password** values for either an Administrator or a Device Manager User to log on.
 - For Administrator, **apc** is the default for **User Name** and **Password**.
 - For Device Manager, **device** is the default for **User Name**, and **apc** is the default for **Password**.

3. Use the **get** command to transmit the text version of the event or data log to your local drive.

```
ftp>get event.txt
```

or

```
ftp>get data.txt
```

4. You can use the **del** command to clear the contents of the event or data log.

```
ftp>del event.txt
```

or

```
ftp>del data.txt
```



You will not be asked to confirm the deletion.

Note

- If you clear the data log, a Deleted Log event will be recorded in the Event Log.
 - If you clear the event log, a new *event.txt* file will be created to record the Deleted Log event.
5. Type `quit` at the `ftp>` prompt to exit from FTP.

Event Actions (Web Interface Only)

Overview

The **Actions** option is available only on the Web interface's **Events** menu. This option allows you to select which actions will occur for events that have a specified severity level:

- **Event Log** selects which severity levels cause an event to be recorded in the event log.



See [Event log action](#).

- **Syslog** selects which severity levels cause messages to be sent to Syslog servers to log events.



See [Syslog action](#).

- **SNMP Traps** selects which severity levels cause SNMP traps to be generated.



See [SNMP traps action](#).

- **Email** selects which severity levels cause e-mail notifications to be sent.



See [Email action](#).

Click **Details** to access a complete list of the System (embedded management card) and Device (Rack PDU) events that can occur, and then edit the actions that will occur for an individual event, as described in [How to Configure Individual Events](#). Click **Hide Details** to return to the **Actions** option.



Note

Modifying events on the **Configure Event Action by Severity Level** page overrides any changes you made to individual events on the **Details** page.

Severity levels

Except for some System (embedded management card) events that do not have a severity level, events are assigned a default severity level based on their seriousness:

- **Informational:** Indicates an event that requires no action, such as a notification of a return from an abnormal condition.
- **Warning:** Indicates an event that may need to be addressed if the condition continues, but does not require immediate attention.
- **Severe:** Indicates an event that requires immediate attention. Unless resolved, severe Device and System events can cause incorrect operation of the Rack PDU or its embedded management card.

Event log action

You can disable the recording of events in the event log. By default, all events are recorded, even events that have no severity level assigned.



Note

Even if you disable the event log action for all severity levels, System (embedded management card) events that have no severity level assigned will still be logged.



For more information about this log, see [Event Log](#).

Syslog action

By default, the **Syslog** action is enabled for all events that have a severity level. However, before you can use this feature to send Syslog messages when events occur, you must configure it.



See [Syslog](#).

SNMP traps action

By default, the **SNMP Traps** action is enabled for all events that have a severity level assigned. However, before you can use SNMP traps for event notifications, you must identify the NMSs (by their IP addresses or domain names) that will receive the traps.



To define up to four NMSs as trap receivers, see [Event Recipients](#).

Email action

By default, the **Email** action is enabled for all events that have a severity level assigned. However, before you can use e-mail for event notifications, you must define the e-mail recipients.



See [E-mail Feature](#).

Event Recipients

Overview

The Web interface and control console both have options that allow you to define up to four trap receivers and up to four e-mail addresses to be used when an event occurs that has SNMP traps or e-mail enabled.



See [Event Actions \(Web Interface Only\)](#).

Trap Receiver settings

To access the **Trap Receiver** settings that allow you to define which NMSs will receive traps:

- In the Web interface, use the **Recipients** option in the **Events** menu.
- In the control console, use the **SNMP** option in the **Network** menu.

| Item | Definition |
|---|--|
| Community Name | This setting defines the password (maximum of 15 characters) used when traps are sent to the NMS identified by the Receiver NMS IP/Domain Name setting. |
| Receiver NMS IP/Domain Name | Identifies by IP address or domain name the NMS that will receive traps. If this setting is 0.0.0.0 (the default value), traps will not be sent to any NMS. |
| Generation (Web interface) Trap Generation (control console) | Enables (by default) or disables the sending of any traps to the NMS identified by the Receiver NMS IP/Domain Name setting. |
| Authentication Traps | Enables or disables the sending of authentication traps to the NMS identified by the Receiver NMS IP/Domain Name setting. |

E-mail Feature

Overview

You can use the Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs.

To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and secondary Domain Name System (DNS) servers



See [DNS servers](#).

- The DNS name of the SMTP server and the **From Address** setting for SMTP



See [SMTP settings](#).

- The e-mail addresses for a maximum of four recipients.



See [Email Recipients](#).



Note

You can use the **To Address** setting of the **Email Recipients** option to send e-mail to a text-based pager.

DNS servers

The Rack PDU cannot send any e-mail messages unless the IP address of the primary DNS server is defined.



See [DNS](#).

The Rack PDU will wait a maximum of 15 seconds for a response from the primary or (if specified) the secondary DNS server. If the Rack PDU does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers that are on the same segment as the Rack PDU or on a nearby segment (but not across a WAN).

Once you define the IP addresses of the DNS servers, verify that DNS is working correctly. Enter the DNS name of a computer on your network to test whether you can look up the IP address for that DNS name.

SMTP settings

The **Email** option in the **Network** menu accesses the following settings:

| Setting | Description |
|--------------|---|
| SMTP Server | Defines the SMTP server by its DNS name. NOTE: This definition is required only when the SMTP Server option (see Email Recipients) is set to Local . |
| From Address | Defines the contents of the From field in the e-mail messages sent by the Rack PDU. NOTE: The SMTP server's configuration may require that you use a valid user account on the server for this setting. See the server's documentation for more information. |

Email Recipients

In the Web interface, use the **Recipients** option in the **Events** menu or the **Configure the Email recipients** link in the “Email Configuration” page to identify up to four e-mail recipients. Use the **Email Test** option to send a test message to a configured recipient.

In the control console, use the **Email** option in the **Network** menu to access the e-mail recipient settings.

| Setting | Description |
|------------|---|
| To Address | <p>Defines the user and domain names of the recipient.</p> <ul style="list-style-type: none">• To bypass the DNS lookup of the mail server’s IP address, use the IP address in brackets instead of the e-mail domain name. For example, use <code>jsmith@[xxx.xxx.xxx.xxx]</code> instead of <code>jsmith@company.com</code>. This is useful when DNS lookups are not working correctly.• To use e-mail for paging, use the e-mail address for that recipient’s pager gateway account (for example, <code>myacct100@skytel.com</code>). The pager gateway pages the recipient. The recipient’s pager must be able to use text-based messaging. |

| Setting | Description |
|-------------|---|
| SMTP Server | <p>Selects one of the following methods for routing e-mail:</p> <ul style="list-style-type: none"> • Through the SMTP server provided with the Rack PDU (the recommended option, Local). This option ensures that the e-mail is sent before the 20-second time-out for the Rack PDU, and, if necessary, is retried several times. Also do one of the following: <ul style="list-style-type: none"> • Enable forwarding at the SMTP server provided with the Rack PDU so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Always check with the administrator of your SMTP server before changing its configuration to allow forwarding. • Set up a special e-mail account for the Rack PDU to forward e-mail to an external mail account. • Directly to the recipient's SMTP server (the Recipient's option). On a busy remote SMTP server, the time-out may prevent some e-mail from being sent, and with this option the Rack PDU tries to send the e-mail only once. <p>When the recipient uses the SMTP server provided with the Rack PDU, the Recipient's setting has no effect.</p> |
| Generation | Enables (by default) or disables sending e-mail to the recipient. |
| Format | <p>Selects the format used for e-mail messages:</p> <p>Short: Identifies only the event that occurred. For example: Switched Rack PDU: Overload threshold exceeded</p> <p>Long: Includes information about the Rack PDU and the event. For example:</p> <p>Name: TestLab Location: Building 3 Contact: DonAdams http://139.225.6.133</p> <p>Switched Rack PDU Ser #: WS0131005294 Date: 6/25/2004 Time: 16:09:48 Code: 0x0F0E</p> <p>Warning - Switched Rack PDU: Overload threshold exceeded</p> |

How to Configure Individual Events

Event List page

The **Actions** option in the **Events** menu opens the “Event Action Configuration” page on the Web interface. Use the **Details** button in this page to access a complete list of the events that can be reported by your Switched Rack PDU.



Note

Modifying events on the **Configure Event Action by Severity Level** page will override any changes you have made to individual events on the **Details** page.

Each event is identified by its unique code, its description, and its assigned severity level. For example:

| Code | Description | Severity |
|--------|--|----------|
| 0x0002 | System: Warmstart. | Severe |
| 0x0F0A | Switched Rack PDU: Low load threshold exceeded | Warning |



For information about severity levels and how they define the actions associated with events, see [Event Actions \(Web Interface Only\)](#).

Detailed Event Action Configuration page

The event codes provide a link to a page that allows you to do the following:

- Change the selected event’s severity level
- Enable or disable whether the event uses the event log, Syslog messages, SNMP traps, or e-mail notifications

Data Menu (Web Interface Only)

Log Option

Use this option to access a log that stores information about the Switched Rack PDU:

- **lout**: The power being output by the Rack PDU.
- **loutmax**: The maximum power output by the Rack PDU since its output power was last recorded.
- **loutmin**: The minimum power output by the Rack PDU since its output power was last recorded.

Use the **Data** menu's **Configuration** option to define how frequently data is sampled and stored in the data log. Each entry is listed by the date and time the data was recorded, and provides the data in a column format.



See [Configuration Option](#).

To retrieve the data log as a text file, see [How to use FTP or SCP to retrieve a log file](#).

Configuration Option

Use this option to access the “Data Log Configuration” page, which reports how much data can be stored in the data log. If you change the **Log Interval** setting, which defines how often data will be sampled and recorded in the data log, the report updates based on the new setting.

The minimum interval is **60** seconds; the maximum interval is **18** hours, **12** minutes, **15** seconds.

Network Menu

Introduction

Overview

Use the **Network** menu to do the following tasks:

- Define TCP/IP settings, including DHCP or BOOTP server settings, when one of those types of servers is used to provide the required TCP/IP values
- Use the Ping utility
- Define and display settings that affect the Switched Rack PDU's settings for DNS, FTP, Telnet, SSH, SNMP, E-mail, Syslog, and the Web interface (SSL/TLS)



Note

Only an Administrator has access to the **Network** menu.

Menu options

Unless noted, the following options are available in the control console and Web interface:

- TCP/IP
- DNS
- Send DNS Query (Web interface)
- Ping utility (control console only)
- FTP Server
- Telnet/SSH
- SNMP
- Email
- Syslog
- Web/SSL (Web/SSL/TLS in the control console)
- WAP
- ISX Protocol (control console only)

Option Settings

TCP/IP

This option accesses the following settings:

- A Boot mode setting selects the method used to define the TCP/IP values that a Rack PDU needs to operate on the network:
 - The IP address of the Rack PDU
 - The subnet mask value
 - The IP address of the default gateway



For information about the watchdog role of the default gateway, see [Resetting the network timer](#).



See also

For information about how to configure the initial TCP/IP settings when you install the Rack PDU, see the *Installation and Quick Start* manual (`.\doc\en\insguide.pdf`), provided on the APC Rack PDU *Utility* CD that came with your Rack PDU and as a printed manual.

- [Advanced settings](#) define the Rack PDU's host and domain names, as well as TCP/IP port, BOOTP, and DHCP settings used by the Rack PDU.

Current TCP/IP settings fields. The current values for **System IP**, **Subnet Mask**, and **Default Gateway**, and the Rack PDU's **MAC Address**, **Host Name**, **Domain Name**, and **Ethernet Port Speed** values are displayed above the TCP/IP settings in the control console and the Web interface.

Boot mode setting. This setting selects which method will be used to define the Rack PDU's TCP/IP settings whenever the Rack PDU turns on, resets, or restarts:

- **Manual:** Three settings (**System IP**, **Subnet Mask**, and **Default Gateway**), which are available only when **Manual** is used to define the needed TCP/IP settings.
- **BOOTP only:** A BOOTP server provides the TCP/IP settings.
- **DHCP only:** A DHCP server provides the TCP/IP settings.
- **DHCP & BOOTP:** The Rack PDU will attempt to get its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server.



Note

An **After IP Assignment** setting, by default, will switch **Boot mode** from its default **DHCP & BOOTP** setting to **BOOTP only** or **DHCP only**, depending on the type of server that supplied the TCP/IP settings to the Rack PDU.



For information about the **After IP Assignment** setting, and other settings that affect how the Rack PDU uses BOOTP and DHCP, see [Advanced settings](#).

Advanced settings. The boot mode affects which settings are available:

- Two settings are available for all **Boot mode** selections to define the Rack PDU's **Host Name** and **Domain Name** values.
 - **Host Name:** When an Administrator configures a host name here and a domain name in the **Domain Name** field, users can then enter a host name in any field in the Switched Rack PDU interface (except e-mail addresses) that accepts a domain name as input.
 - **Domain Name:** An Administrator needs to configures the domain name here only. In all other fields in the Switched Rack PDU interface (except e-mail addresses) that accept domain names, the

Rack PDU will add this domain name when only a hostname is entered.



Note

To override the expansion of a specified host name by the addition of the domain name, do one of the following:

- To override the behavior in all instances, set the domain name field in **Configure General Settings** to its default `somedomain.com` or to `0.0.0.0`.
 - To override the behavior for a particular host name entry — for example when defining a trap receiver — include a trailing period. The Switched Rack PDU recognizes a host name with a trailing period (such as *mySnmpServer.*) as if it were a fully qualified domain name and therefore does not append the domain name.
- A **Port Speed** setting is available for all **Boot mode** selections to define the TCP/IP port's communication speed (**Auto-negotiate**, by default).
 - Three settings are available for all **Boot mode** selections, except **Manual**, to identify the Rack PDU in BOOTP or DHCP communication:
 - **Vendor Class**: Uses **APC**, by default.
 - **Client ID**: Uses the Rack PDU's MAC address, by default.



Caution

If the **Client ID** is changed from the Rack PDU's MAC address, the new value must be unique on the LAN.

Otherwise, the DHCP or BOOTP server may act incorrectly.

- **User Class**: Uses the Rack PDU's application module type, by default.

- Two settings are available if **BOOTP only** is the Boot mode selection:
 - **Retry Then Fail**: Defines how many times the Rack PDU will attempt to discover a BOOTP server before it stops (4, by default).

- **On Retry Failure:** Defines what TCP/IP settings will be used by the Rack PDU when it fails to discover a BOOTP server (**Use Prior Settings**, by default).



For information about the **Advanced** settings (**DHCP Cookie Is** and **Retry Then Stop**) that directly affect how DHCP is used, see **Boot Mode**.

DNS

Configure Domain Name System Settings fields. Use these fields to define the IP addresses of the primary and secondary Domain Name System (DNS) servers used by the Switched Rack PDU e-mail feature.



See **E-mail Feature** and **DNS servers**.

Send DNS Query (Web interface). Use this option, available only through the **DNS** menu in the Web interface, to send a DNS query that tests the setup of your DNS servers.

Use the following settings to define the parameters for the test DNS request; you view the result of the test DNS request in the **Last Query Response** field (which displays **No last query** or text describing the query result of the last test).

- Use the **Query Type** setting to select the method to use for the DNS query:
 - The URL name of the server (**Host**)
 - The IP address of the server (**IP**)
 - The fully qualified domain name (**FQDN**)
 - The Mail Exchange used by the server (**MX**)
- Use the **Query Question** text field to identify the value to be used for the selected **Query Type**:

- For **Host**, identify the URL
- For **IP**, identify the IP address
- For **FQDN**, identify the fully qualified domain name, formatted as *myserver.mydomain.com*.
- For **MX**, identify the Mail Exchange address
- Enable or disable **Reverse DNS Lookup**, which is disabled by default. Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic. With **Reverse DNS Lookup** enabled, when a network-related event occurs, reverse DNS lookup logs in the event log both the IP address and the domain name for the networked device associated with the event. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change much less frequently than IP addresses, enabling reverse DNS lookup can improve the ability to identify addresses of networked devices that are causing events to occur.

Ping utility (control console only)

Select this option, available only in the control console, to check the network connection by testing whether a defined IP address or domain name responds to the Ping network utility.

By default, the IP address of the default gateway is used. However, you can use the IP address or domain name of any device known to be running on the network.

FTP Server

Use the **Access** setting to enable or disable the FTP server. The server is enabled by default.



Note

FTP transfers files without using encryption. For higher security, use Secure CoPy (SCP) for file transfers. When you select and configure Secure Shell (SSH), SCP is enabled automatically. To configure SSH, see [Telnet/SSH](#). If you decide to use SCP for file transfer, be sure to disable the FTP server.

Use the **Port** setting to identify the TCP/IP port that the FTP server uses for communications with the Rack PDU. The default **Port** setting is **21**.

You can change the **Port** setting to any unused port from **5000** to **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port. For example, for a port number of 5000 and a Rack PDU IP address of 159.215.12.114, you would use this command:

```
ftp 159.215.12.114:5000
```



To access a text version of the Rack PDU's event or data log, see [How to use FTP or SCP to retrieve a log file](#).

Telnet/SSH

Use the **Telnet/SSH** option to perform the following tasks:

- Enable or disable Telnet or the Secure Shell (SSH) protocol for remote control console access.
 - While SSH is enabled, you cannot use Telnet to access the control console.
 - Enabling SSH enables SCP automatically.



Note

When SSH is enabled and its port and encryption ciphers configured, no further configuration is required to use SCP. (SCP uses the same configuration as SSH.)

- Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)



Note

To use SSH, you must have an SSH client installed. Most Linux and other UNIX[®] platforms include an SSH client as part of their installation, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

- Configure the port settings for Telnet and SSH.
- Select one or more data encryption algorithms for SSH version 1, SSH version 2, or both.
- In the Web interface, specify a host key file previously created with the APC Security Wizard and load it to the Rack PDU.

From a command line interface, such as the command prompt on Windows operating systems, you can use FTP or Secure CoPy (SCP) to transfer the host key file. You must transfer the file to location `/sec` on the Rack PDU.



Note

If you do not specify a host key file, the Switched Rack PDU generates an RSA host key of 768 bits, instead of the 1024-bit RSA host key that the Wizard creates. **The Rack PDU can take up to 5 minutes to create this host key, and SSH is not accessible during that time.**

- Display the *fingerprint* of the SSH host key for SSH versions 1 and 2. Most SSH clients display the fingerprint at the start of a session. Compare the fingerprint displayed by the client to the fingerprint that you recorded from the Web interface or control console of the Rack PDU.



Note

If you are using SSH version 2, expect a noticeable delay when logging on to the control console of the Rack PDU. Although the delay is not long, it can be mistaken for a problem because there is no explanatory message.

| Option | Description |
|---|--|
| Telnet/SSH Network Configuration | |
| Access | Enables or disables the access method selected in Protocol Mode . NOTE: Enabling SSH automatically disables Telnet. To enable SSH, change the setting and then click Next>> in the Web interface or choose Accept Changes in the control console. You must then agree to the license agreement that is displayed. |
| Protocol Mode | Choose one of the following: <ul style="list-style-type: none">• Telnet: User names, passwords, and data are transmitted without encryption.• Secure SHell (SSH), version 1: User names, passwords, and data are transmitted in encrypted form. There is little or no delay when you are logging on.• Secure SHell (SSH), version 2: User names, passwords, and data are transmitted in encrypted form, but with somewhat more protection than version 1 from attempts to intercept, forge, or alter data during data transmission. There is a noticeable delay when you are logging on to the Rack PDU.• Secure SHell (SSH), versions 1 and 2: Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.) |

| Option | Description |
|--------------------------------------|---|
| Telnet/SSH Port Configuration | |
| Telnet Port | <p>Identifies the TCP/IP port used for communications by Telnet with the Rack PDU. The default is 23.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings. Then, according to the requirements of your Telnet client program, you must use either a colon (:) or a space in the command line to specify the non-default port number. For example, for a port number of 5000 and a Rack PDU IP address of 159.215.12.114, your Telnet client would require one or the other of the following commands:</p> <pre>telnet 159.215.12.114:5000 telnet 159.215.12.114 5000</pre> |
| SSH Port | <p>Identifies the TCP/IP port used for communications by the Secure Shell (SSH) protocol with the Rack PDU. The default is 22.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings. See the documentation for your SSH client for information on the command line format required to specify a non-default port number when starting SSH.</p> |

| Option | Description |
|---------------------------------|---|
| SSH Server Configuration | |
| SSHv1 Encryption Algorithms | <p>Enables or disables DES, and displays the status (always enabled) of Blowfish, two encryption algorithms (block ciphers) compatible with SSH, version 1, clients.</p> <ul style="list-style-type: none"> • DES: The key length is 56 bits. • Blowfish: The key length is 128 bits. You cannot disable this algorithm. <p>NOTE: Not all SSH clients can use every algorithm. If your SSH client cannot use Blowfish, you must also enable DES.</p> |
| SSHv2 Encryption Algorithms | <p>Enables or disables the following encryption algorithms (Block Ciphers) that are compatible with SSH version 2 clients.</p> <ul style="list-style-type: none"> • 3DES (enabled by default): The key length is 168 bits. • Blowfish (enabled by default): The key length is 128 bits. • AES 128: The key length is 128 bits. • AES 256: The key length is 256 bits. <p>NOTE: Not all SSH clients can use every algorithm. Your SSH client selects the algorithm that provides the highest security from among the enabled algorithms that it is able to use. (If your SSH client cannot use either of the default algorithms, you must enable an AES algorithm that it can use.)</p> |

| Option | Description |
|-------------------------------|--|
| SSH User Host Key File | |
| Status: | <p>The Status field indicates the status of the host key (<i>private</i> key). In the control console, you display host key status by selecting Advanced SSH Configuration.</p> <ul style="list-style-type: none"> • SSH Disabled: No host key in use: No host key has been transferred to the Rack PDU, or a host key has been transferred improperly. <p>NOTE: A host key must be installed to the /sec directory of the Rack PDU.</p> <ul style="list-style-type: none"> • Generating: The Rack PDU is generating a host key because no valid host key was installed in its /sec directory. • Loading: A host key is being loaded (i.e., being activated on the Rack PDU). • Valid: The host key is valid. (If you install an invalid host key, the Rack PDU discards it and generates a valid one. However, a host key that the Rack PDU generates is only 768 bits in length. A valid host key created by the APC Security Wizard is 1024 bits.) |
| Filename: | <p>You can create a host key file with the APC Security Wizard and then upload it to the Rack PDU by using the Web interface. Use the Browse button for the Filename field to locate the file, then click Apply.</p> <p>Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the Rack PDU.</p> <p>NOTE: Creating and uploading a host key in advance reduces the time required to enable SSH. If no host key is loaded when you enable SSH, the Rack PDU creates one when it reboots. The Rack PDU takes up to 5 minutes to create this key, and the SSH server is not accessible during that time.</p> |

| Option | Description |
|---------------------------------|---|
| SSH Host Key Fingerprint | |
| SSH v1: | Displays the SSH version 1 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose Advanced SSH Configuration and then Host Key Information to display the fingerprint. |
| SSH v2: | Displays the SSH version 2 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose Advanced SSH Configuration and then Host Key Information to display the fingerprint. |

SNMP

An **Access** option (the **Settings** option in the control console) enables (by default) or disables SNMP. When SNMP is enabled, the **Access Control** settings allow you to control how each of the four available SNMP channels is used.



To define up to four NMSs to serve as trap receivers, see **Trap Receiver settings**.



See also

To use SNMP to manage a Switched Rack PDU, see the *PowerNet[®] SNMP Management Information Base (MIB) Reference Guide* (.doc\en\mibguide.pdf) on the APC Rack PDU *Utility* CD that came with your Rack PDU.

| Setting | Definition |
|----------------|--|
| Community Name | Defines the password (maximum of 15 characters) that an NMS defined by the NMS IP/Domain Name setting uses to access the channel. |

| Setting | Definition | |
|---------------------------|---|---|
| NMS IP/ Domain Name | Limits access to the NMS specified by a domain name or to the NMSs specified by the format used for the IP address: <ul style="list-style-type: none"> • A domain name allows only the NMS at that location to have access. • 159.215.12.1 allows only the NMS with that IP address to have access. • 159.215.12.255 allows access for any NMS on the 159.215.12 segment. • 159.215.255.255 allows access for any NMS on the 159.215 segment. • 159.255.255.255 allows access for any NMS on the 159 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS. | |
| Access Type | Selects how the NMS defined by the NMS IP setting can use the channel when that NMS uses the correct value for Community Name . | |
| | Read | The NMS can use GETs at any time, but it can never use SETs. |
| | Write | The NMS can use GETs at any time, and can use SETs when no one is logged on to either the control console or Web interface. |
| | Disabled | The NMS cannot use GETs or SETs. |
| | Write+ | The NMS can use GETs and SETs at any time, even when someone is logged on to the control console or Web interface. |

Email

Use this option to define two SMTP settings (**SMTP Server** and **From Address**) used by the e-mail feature of the Switched Rack PDU.



See [SMTP settings](#) and [E-mail Feature](#).

An **Access** option (the **Settings** option in the control console) enables (by default) or disables SNMP. When SNMP is enabled, the **Access Control** settings allow you to control how each of the four available SNMP channels is used.

Syslog

By default, the Rack PDU can send messages to up to four Syslog servers whenever System (embedded management card) and Switched Rack PDU (Device) events occur. The Syslog servers, which must be specifically identified by their IP addresses or domain names, record the events in a log that provides a centralized record of events that occur at network devices.



See also

This user's guide does not describe Syslog or its configuration values in detail. For more information about Syslog, see RFC3164, at www.ietf.org/rfc/rfc3164.

Syslog settings. Leave the Syslog settings, except the **Server IP** settings, set to their defaults unless otherwise specified by the Syslog network or system administrator.

| Setting | Definition |
|-------------------------|---|
| General Settings | |
| Syslog | Enables (by default) or disables the Syslog feature. |
| Facility | Selects the facility code assigned to the Rack PDU's Syslog messages (User , by default). NOTE: Although several daemon-specific and process-specific selections are available, along with eight generic selections, User is the selection that best defines the Syslog messages sent by a Rack PDU. |

| Setting | Definition |
|--|---|
| Syslog Server Settings | |
| Server IP/ Domain Name | <p>Uses specific IP addresses or domain names to identify which of up to four servers will receive Syslog messages sent by the Rack PDU.</p> <p>NOTE: To use the Syslog feature, at least Server IP/Domain Name must be defined for at least one server.</p> |
| Port | <p>Identifies the user datagram protocol (UDP) port that the Rack PDU will use to send Syslog messages. The default is 514, the number of the UDP port assigned to Syslog.</p> |
| Local Priority (Severity Mapping) | |
| Map to Syslog's Priorities | <p>Maps each of the severity levels (Local Priority settings) that can be assigned to System and Rack PDU events to the available Syslog priorities. The following definitions are from RFC3164:</p> <ul style="list-style-type: none"> • Emergency: The system is unusable • Alert: Action must be taken immediately • Critical: Critical conditions • Error: Error conditions • Warning: Warning conditions • Notice: Normal but significant conditions • Informational: Informational messages • Debug: Debug-level messages <p>Following are the default settings for the four Local Priority settings:</p> <ul style="list-style-type: none"> • Severe is mapped to Critical. • Warning is mapped to Warning. • Informational is mapped to Info. • None (for events that have no severity level assigned) is mapped to Info. <p>NOTE: To disable sending Syslog messages for Severe, Warning, or Informational events, see Event Actions (Web Interface Only).</p> |

Syslog test (Web interface). This option allows you to send a test message to the Syslog servers configured in the **Syslog Server** section.

1. For **Priority**, select the priority to assign to the test message.
2. For **Test Message**, use any text that meets the format described in **Syslog message format** — for example, `APC: Test message`.
3. Click **Apply** to have the Rack PDU send a Syslog message that uses the defined **Priority** and **Test Message** settings.

Syslog message format. A Syslog message has three parts:

- The priority (PRI) part identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the Rack PDU.
- The header includes a time stamp and the IP address of the Rack PDU.
- The message (MSG) part has two fields:
 - A TAG field, which is followed by a colon and a space, identifies the event type (System, or Device, for example).
 - A CONTENT field provides the event text, followed by a space and the event code.

Web/SSL (Web/SSL/TLS in the control console)

Use the **Web/SSL** menu to perform the following tasks.

- Enable or disable the two protocols that provide access to the Web interface of the Switched Rack PDU:
 - Hypertext Transfer Protocol (HTTP) provides access by user name and password, but does not encrypt user names, passwords, and data during transmission.
 - Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS). Secure Sockets Layer (SSL) encrypts user names, passwords, and data during transmission and provides authentication of the Switched Rack PDU by means of digital certificates.



See [Creating and Installing Digital Certificates](#) to choose among the several methods for using digital certificates.


- Configure the ports that each of the two protocols will use.
- Select the encryption ciphers that SSL will use.
- Identify whether a server certificate is installed on the Rack PDU. If a certificate has been created with the APC Security Wizard but is not installed:
 - In the Web interface, browse to the certificate file and upload it to the Rack PDU.
 - Alternatively, use the Secure CoPy (SCP) protocol or FTP to upload it to the location `\sec` on the Rack PDU.



Note

Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Rack PDU creates one when it reboots. **The Rack PDU can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.**

- Display the configured parameters of a digital server certificate, if one is installed.

| Option | Description |
|--------------------------------------|---|
| Web/SSL Network Configuration | |
| Access | Enables or disables the access method selected in Protocol Mode . |
| Protocol Mode | <p>Choose one of the following:</p> <ul style="list-style-type: none"> • HTTP: User names, passwords, and data are transmitted without encryption. • HTTPS (SSL/TLS): User names, passwords, and data are transmitted in encrypted form, and digital certificates are used for authentication. <p>NOTE: To enable HTTPS (SSL/TLS), change the setting and then click Next>> in the Web interface, or choose Accept Changes in the control console. You must then agree to the license agreement that is displayed. To activate the changes you must log off and log back on to the interface. When SSL is activated, your browser displays a lock icon, usually at the bottom of the screen.</p>  |

| Option | Description |
|--------------------------------------|---|
| HTTP/HTTPS Port Configuration | |
| HTTP Port | <p>Identifies the TCP/IP port used for communications by HTTP with the Rack PDU. The default is 80.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings.</p> <p>You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5000 and a Rack PDU IP address of 159.215.12.114, you would use this command:</p> <pre>http://159.215.12.114:5000</pre> |
| HTTPS Port | <p>Identifies the TCP/IP port used for communications by HTTPS with the Rack PDU. The default is 443.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings.</p> <p>You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 6502 and a Rack PDU IP address of 159.215.12.114, you would use this command:</p> <pre>https://159.215.12.114:6502</pre> |

| Option | Description |
|-------------------------------------|---|
| SSL/TSL Server Configuration | |
| CipherSuite | <p>Enables or disables the following SSL encryption ciphers and hash algorithms. (To access these options in the control console, choose Web/SSL, then Advanced SSL/TLS Configuration.)</p> <p>NOTE: All of these encryption ciphers and hash algorithms use the RSA public key algorithm.</p> <ul style="list-style-type: none"> • DES (SSL_RSA_WITH_DES_CBC_SHA): a block cipher with a key length of 56 bits. The Secure Hash Algorithm (SHA) is used for authentication. • 3DES (SSL_RSA_WITH_3DES_EDE_CBC_SHA): a block cipher with a key length of 168 bits. A Secure Hash Algorithm (SHA) is used for authentication. • RC4 (SSL_RSA_WITH_RC4_128_MD5): a stream cipher with a key length of 128 bits, with an RSA key exchange algorithm, and with a Message Digest 5 (MD5) hash algorithm used for authentication. This selection is enabled by default. • RC4 (SSL_RSA_WITH_RC4_128_SHA): a stream cipher with a key length of 128 bits. A Secure Hash Algorithm (SHA) is used for authentication. This selection is enabled by default. |

| Option | Description |
|-----------------------------------|---|
| SSL/TLS Server Certificate | |
| Status: | <p>The Status field indicates whether a server certificate is installed. (To display the status in the control console, choose Web/SSL/TLS, then Advanced SSL/TLS Configuration.)</p> <ul style="list-style-type: none"> • Not installed: No certificate is installed on the Rack PDU. <p>NOTE: If you install a certificate by using FTP or SCP, you must specify the correct location (/sec) on the Rack PDU.</p> <ul style="list-style-type: none"> • Generating: The Rack PDU is generating a certificate because no valid certificate was installed. • Loading: A certificate is being loaded (activated on the Rack PDU). • Valid: A valid certificate was installed to or generated by the Rack PDU. (If you install an invalid certificate, the Rack PDU discards it and generates a valid one. However, a certificate that the Rack PDU generates has some limitations. See Method 1: Use the auto-generated default certificate.) |
| Filename: | <p>You can create a server certificate with the APC Security Wizard and then upload it to the Rack PDU by using the Web interface. Use the Browse button for the Filename field to locate the file, then click Apply. By default, the certificate is installed to the correct location.</p> <p>Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Rack PDU. However, you must specify the correct location (/sec) on the Rack PDU.</p> <p>NOTE: Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Rack PDU creates one when it reboots. The Rack PDU can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.</p> |

| Parameter | Description |
|------------------------------------|--|
| Current Certificate Details | |
| Issued to: | <p>Common Name (CN): The IP Address or DNS name of the Rack PDU, except if the server certificate was generated by default by the Rack PDU. For a default server certificate, the Common Name (CN) field displays the Rack PDU's serial number.</p> <p>NOTE: If an IP address was specified as the Common Name when the certificate was created, use an IP address to log on to the Web interface of the Rack PDU; if the DNS name was specified as the Common Name, use the DNS name to log on. When you log on, if you do not use the IP address or DNS name that was specified for the certificate, authentication fails, and you receive an error message asking if you want to continue.</p> <p>Organization (O), Organizational Unit (OU), and Locality, Country: The name, organizational unit, and location of the organization that is using the server certificate. If the server certificate was generated by default by the Rack PDU, the Organizational Unit (OU) field displays "Internally Generated Certificate."</p> <p>Serial Number: The serial number of the server certificate.</p> |
| Issued By: | <p>Common Name (CN): The Common Name as specified in the CA root certificate, except if the server certificate was generated by default by the Rack PDU. For a default server certificate, the Common Name (CN) field displays the Rack PDU's serial number.</p> <p>Organization (O) and Organizational Unit (OU): The name and organizational unit of the organization that issued the server certificate. If the server certificate was generated by default by the Rack PDU, the Organizational Unit (OU) field displays "Internally Generated Certificate."</p> |
| Validity: | <p>Issued on: The date and time at which the certificate was issued.</p> <p>Expires on: The date and time at which the certificate expires.</p> |

| Parameter | Description |
|--------------|---|
| Fingerprints | <p>Each fingerprint is a long string of alphanumeric characters punctuated by colons. A fingerprint is a unique identifier that you can use to further authenticate the server. Record the fingerprints to compare with the fingerprints contained in the certificate, as displayed in the browser.</p> <p>SHA1 Fingerprint: This fingerprint is created by a Secure Hash Algorithm (SHA).</p> <p>MD5 Fingerprint: This fingerprint is created by a Message Digest 5 (MD5) algorithm.</p> |

WAP

Use this option to disable (the default) or enable the Wireless Application Protocol (WAP). WAP is a standard for providing cellular phones, pagers and other handheld devices with secure access to e-mail and text-based Web pages. WAP runs on all major wireless networks and is device-independent, so that it can be used with many phones and handheld devices.

ISX Protocol (control console only)

Use this option to enable (the default) or disable the APC InfraStruXure (ISX) Protocol. The APC InfraStruXure (ISX) Protocol allows the Switched Rack PDU to communicate with other APC devices, including the InfraStruXure Manager, if your system includes one.

System Menu

Introduction

Overview

Use the **System** menu to do the following tasks:

- Configure system identification, date and time settings, and Administrator, Read-Only User, Device manager, and Outlet User access
- Centrally administer remote access for each Rack PDU by using RADIUS (Remote Authentication Dial-in User Service)
- Synchronize the real-time clock for the Rack PDU with a Network Time Protocol (NTP) server
- Reset the Rack PDU to default settings
- Define the URL links available in the Web interface (configurable through the Web interface only)
- Access hardware and firmware information about the Rack PDU (control console only)
- Download configuration files (control console only)



Note

Only an Administrator has access to the **System** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- [User Manager](#)
- [Outlet User Manager](#)
- [RADIUS](#)
- [Identification](#)
- [Date & Time](#)
- [Tools](#)
- [Links \(Web interface\)](#)
- [Modem \(not supported\)](#)
- [About System](#)



Note

The **About System** option is a **Help** menu option in the Web interface.

Option Settings

User Manager

Use this option to define access values shared by the control console and Web interface.

| Setting | Definition |
|--|--|
| Values affecting all users | |
| Auto Logout | The number of minutes (3, by default) before a user is automatically logged off because of inactivity. |
| Separate values for Administrator, Device Manager, and Read Only User | |
| User Name | The case-sensitive name (maximum of 10 characters) used to log on at the control console or Web interface, and by the Read Only User to log onto the Web interface only. <ul style="list-style-type: none">• apc, by default, for Administrator• device, by default, for Device Manager User• readonly, by default, for Read Only User |
| Password | The case-sensitive password (maximum of 10 characters) always used to log on at the control console, but used to log into the Web interface only when Basic is selected for the Authentication setting (apc is the default for the Password settings for all account types). NOTE: A Read-Only User is not permitted to log on through the control console. |

Outlet User Manager

Use the **Outlet User Manager** option to set up user accounts that have access only to specified outlets.

Web interface. Choose a user name, or choose **Add New User** to edit accounts.

| Setting | Definition |
|------------------|---|
| User Name | The name of this user account. NOTE: A user name in orange indicates that the user account has been disabled. |
| Password | Case-sensitive password for this user account. |
| User Description | Identification or description of the outlet user. |
| Account Status | Enables or disables this user's account. |
| Outlet Access | Selects the outlets to which users have access. |
| Delete User | Deletes this user account. |

Control console. Select **System** from the **Control Console** menu. Then select **Manage Outlet Users** from the **User Manager** menu.

| Setting | Definition |
|---|---|
| Add Outlet User Account or Edit Outlet User Account | <p>User Name: The user name for logging on to this user account.</p> <p>Password: Case-sensitive password for this user account.</p> <p>Description: Identification of the outlet user.</p> |
| Delete Outlet User Account | Enter the user name of the outlet user account to delete. |
| Disable Outlet User Account | Enter the user name of the outlet user account to disable. |
| Enable Outlet User Account | Enter the user name of the outlet user account to enable. |
| Edit Users Outlet Access | <p>Select the outlets to which users have access:</p> <ol style="list-style-type: none"> 1. Enter the user name of the outlet user account to modify. 2. Select the numbers of the outlets to which the outlet user will have access: <ul style="list-style-type: none"> •To add access to an outlet, enter an outlet number and press ENTER. Enter a space character when you finish adding access to outlets. •To remove access to an outlet, enter an outlet number preceded by a minus sign (-) and press ENTER. Enter a space character when you finish removing access to outlets. |
| List Outlet Users Accounts | Display outlet user name, status, description, and outlet access for each outlet user account. |

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization, and accounting service. APC supports the authentication and authorization functions of RADIUS. Use this option to centrally administer remote access for each Rack PDU.

When a user accesses the Switched Rack PDU, it sends an authentication request to the RADIUS server to determine the user's permission level.



Note

RADIUS user names are limited to 32 characters.



For more information on user permission levels, see [Types of user accounts](#).



Note

The RADIUS server and the Rack PDU must be configured before RADIUS authentication and authorization will operate properly.



Note

RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.

Configuring the Rack PDU.

| RADIUS Setting | Definition |
|--------------------------------|--|
| Access | Local Only: RADIUS is disabled. Local authentication is enabled. |
| | RADIUS then Local: RADIUS is enabled, and local authentication is enabled. Authentication is requested from the RADIUS server first; local authentication is used only if RADIUS authentication fails. |
| | RADIUS Only: RADIUS is enabled. Local authentication is disabled. NOTE: If RADIUS Only is selected, the only way to recover if the RADIUS server is unavailable is by using a serial connection to the control console and changing the Access setting to Local Only or RADIUS then Local . |
| Primary Server | The server name or IP address of the main RADIUS server. |
| Primary Server Secret | The shared secret between the primary RADIUS server and the Rack PDU. |
| Secondary Server | The server name or IP address of the secondary RADIUS server. |
| Secondary Server Secret | The shared secret between the secondary RADIUS server and the Rack PDU. |
| Timeout | The time in seconds that the Rack PDU waits for a response from the RADIUS server. |

Configuring the RADIUS server. You must configure your RADIUS server to work with the Rack PDU. The following example shows how to configure a RADIUS server for use with a Rack PDU. APC supports authentication and authorization of users by various RADIUS servers and does not recommend a specific RADIUS server.

1. Add the IP address of the Rack PDU to the RADIUS server client list (file).
2. The users must be configured with a Service-Type attribute. If no Service-Type attribute is configured, the user will have read-only access (on the Web interface only). There are two acceptable values for Service-Type: Administrative-User (6), which gives the user Administrator permissions, or Login-User (1), which gives the user Device Manager permissions.

The following examples may differ somewhat from the required content or format of your specific RADIUS server.



See also

See your RADIUS server documentation for information about the RADIUS users file.

Example: (RADIUS users file)

```
#
UPSAdmin    Auth-Type = Local, Password = "admin"
            Service-Type = Administrative-User

UPSDevice   Auth-Type = Local, Password = "device"
            Service-Type = Login-User

UPSReadOnly Auth-Type = Local, Password = "readonly"
```

3. Vendor specific attributes (VSA) can also be used. This requires some dictionary entries. VSAs take precedence over standard RADIUS attributes.

Example: (RADIUS, dictionary.apc)

```
#
# dictionary.apc
#
#
VENDOR    APC        318

#
# Attributes
#
ATTRIBUTE APC-Service-Type 1 integer APC
ATTRIBUTE APC-Outlets      2 string  APC

VALUE APC-Service-Type Admin    1
VALUE APC-Service-Type Device   2
VALUE APC-Service-Type ReadOnly 3
VALUE APC-Service-Type Outlet   4
```

Example: (RADIUS users file with VSAs)

```
VSAAdmin    Auth-Type = Local, Password = "admin"
            APC-Service-Type = Admin

VSADevice   Auth-Type = Local, Password = "device"
            APC-Service-Type = Device

VSAReadOnly Auth-Type = Local, Password = "readonly"
            APC-Service-Type = ReadOnly

# Give user access to device outlets 1, 2 and 3.
VSAOutlet   Auth-Type = Local, Password = "outlet"
            APC-Service-Type = Outlet,
            APC-Outlets = "1,2,3"
```



For more information on user permission levels, see [Types of user accounts](#).

Identification

Use this option to define the System **Name**, **Contact**, and **Location** values used by the SNMP agent for the Rack PDU. The option's settings provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).



See also

For more information about the MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide* (.doc\en\mibguide.pdf) provided on the APC Rack Power Distribution Unit *Utility* CD that came with your Rack PDU.

Date & Time

Use this option to set the date and time used by the Switched Rack PDU. The option displays the current settings and allows you to change those settings manually or through a Network Time Protocol (NTP) Server.

Set Manually. Use this option in the Web interface, or **Manual** in the control console, to set **Date** and **Time** for the Switched Rack PDU.



Note

An **Apply Local Computer Time to System** option, which is available in the Web interface only, sets these values to match the date and time settings of the computer you are using to access the Web interface.

Synchronize with Network Time Protocol (NTP) Server. Use this option on the Web interface, or **Network Time Protocol (NTP)** on the control console, to have an NTP Server automatically update the **Date** and **Time** settings for the Switched Rack PDU.



Note

In the control console, use the **NTP Client** option to enable or disable the NTP Server updates. In the Web interface, use the **Set Manually** option. The updates are disabled by default.

| Setting | Definition |
|----------------------|---|
| Primary NTP Server | Identifies the IP address or domain name of the primary NTP server. |
| Secondary NTP Server | Identifies the IP address or domain name of the secondary NTP server when a secondary server is available. |
| Time Zone | Defines the offset to be used from Greenwich Mean Time (GMT) based on the time zone in which the Rack PDU is located. |
| Update Interval | Defines how often, in hours, the Rack PDU will access the NTP Server for an update. The minimum interval is 1 hour and the maximum is 8760 hours (one year). Use Update Using NTP Now to initiate an immediate update as well. |

Tools

Use this option to perform the following actions.

| Action | Definition |
|---|---|
| No Action (Web Interface only) | No change to the Rack PDU. |
| Reboot Management Interface | Restarts the user interface of the Rack PDU. |
| Reset to Defaults | Resets all configuration settings. This option will reset the TCP/IP settings and enable DHCP and BOOTP. |
| Reset to Defaults Except TCP/IP | Resets all configuration settings except the TCP/IP settings. |
| Reset Only TCP/IP to Defaults | Resets the TCP/IP settings only. This option will not enable DHCP and BOOTP. |
| Delete SSH Host Keys and SSL Certificates | Removes all host keys you configured for Secure Shell for encryption-based security at the control console and all certificates that you configured for Secure Sockets Layer for authentication at the Web interface. |
| File Transfer (control console only) | Allows you to select one of the following to transfer firmware files to the Switched Rack PDU. <ul style="list-style-type: none">• XMODEM: A terminal-emulation program that you can use only through a direct serial connection to the Switched Rack PDU.• FTP: File Transfer Protocol (FTP client application).• TFTP: Trivial File Transfer Protocol (TFTP client application). |
| Upload (Web Interface only) | Upload a user configuration file (.ini file) to the Switched Rack PDU. <ul style="list-style-type: none">• To create the file, retrieve settings from a configured Switched Rack PDU. See How to Export Configuration Settings.• To upload the file, in the User Configuration File section specify or browse to the file name, and then click Upload. |

Links (Web interface)

Use this option to modify the links to APC Web pages.

| Setting | Definition |
|---------------------|--|
| User Links | |
| Name | Defines the link names that appear in the Links menu (by default, APC's Web Site , Testdrive Demo , and Remote Monitoring). |
| URL | Defines the URL addresses used by the links. By default, the following URL addresses are used: <ul style="list-style-type: none">• http://www.apc.com (APC's Web site)• http://testdrive.apc.com (Testdrive Demo)• http://rms.apc.com (Remote Monitoring) NOTE: Only links of the type http:// can be used in these fields. For information about these pages see Links menu . |
| Access Links | |
| APC Home Page | Defines the URL address used by the APC logo at the top of all Web interface pages (by default, http://www.apc.com). |

Modem (not supported)

This option, shown only in the control console, is not supported for Rack PDUs.

About System

This option identifies the following hardware information for the Rack PDU: **Model Number**, **Serial Number**, **Hardware Revision**, **Manufacture Date**, and **MAC Address**.

This screen also displays the **Name**, **Version**, **Date**, and **Time** for the Application Module and AOS.

This information is set at the factory and cannot be changed.

The control console also includes fields for system **Flash Type**, and **Type**, **Sector**, and **CRC16** for each module.



Note

In the Web interface, except for **Flash Type**, this hardware information is reported by the **About System** option in the **Help** menu.

Boot Mode

Introduction

Overview

In addition to using a BOOTP server or manual settings, the Switched Rack PDU can use a dynamic host configuration protocol (DHCP) server to provide the settings that it needs to operate on a TCP/IP network.

The method used to provide the network settings for the Rack PDU depends on **Boot mode**, a **TCP/IP** option in the **Network** menu. To use a DHCP server to provide the network assignment for the Rack PDU, **Boot mode** must be set either to **DHCP & BOOTP**, its default setting, or **DHCP only**.



See also

For more details on DHCP and DHCP options, see RFC2131 and RFC2132.

DHCP & BOOTP boot process

When **Boot mode** is set to its default **DHCP & BOOTP** setting, the following occurs when the Switched Rack PDU is started or reset:

1. The Rack PDU makes up to five requests for its network assignment from any BOOTP server. If a valid BOOTP response is received, the Rack PDU starts the network services and sets **Boot mode** to **BOOTP Only**.
2. If the Rack PDU fails to receive a valid BOOTP response after five BOOTP requests, the Rack PDU makes up to five requests for its network assignment from any DHCP server. If a valid DHCP response is received, the Rack PDU starts the network services and sets **Boot mode** to **DHCP Only**.



Note

To configure the Switched Rack PDU so that it always uses the **DHCP & BOOTP** setting for **Boot mode**, enable the **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** option, which is disabled by default.



See [Switched Rack PDU settings](#).

3. If the Switched Rack PDU fails to receive a valid DHCP response after five DHCP requests, it repeats BOOTP and DHCP requests until it receives a valid network assignment. First it sends a BOOTP request every 32 seconds for 12 minutes, then one DHCP request with a timeout of 64 seconds, and so forth.



Note

If a DHCP server responds with an invalid offer (e.g., without the APC Cookie), the Switched Rack PDU accepts the lease from that server on the last request of the sequence and immediately releases that lease. This prevents the DHCP server from reserving the IP Address associated with its invalid offer.



For more information on what a valid response requires, see [DHCP response options](#).

DHCP Configuration Settings

Switched Rack PDU settings

The **TCP/IP** option in the **Network** menu of the Web interface and control console accesses the network settings for the Switched Rack PDU.

Three settings (**Ethernet Port Speed**, **Host Name**, and **Domain Name**) are available regardless of the **TCP/IP** option's **Boot mode** selection, and three settings (**Vendor Class**, **Client ID**, and **User Class**) are available for any **Boot mode** selection except **Manual**.

When **Boot mode** is set to **DHCP & BOOTP**, two options are available:

- **After IP Assignment** in the control console (or **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** in the Web interface): By default, this option switches **Boot mode** to the selection that reflects the server that provided the TCP/IP settings (**DHCP Only** or **BOOTP Only**).
- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.



For more information about the APC cookie, see [DHCP response options](#).

When **Boot mode** is set to **DHCP Only**, two options are available:

- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.



For more information about the APC cookie, see [DHCP response options](#).

- **Retry Then Stop** in the control console (or **Maximum # of Retries** in the Web interface): This option sets the number of times the Switched Rack PDU will repeat the DHCP request if it does not receive a valid response. By default, the number of retries is 0, which sets the Switched Rack PDU to continue repeating the DHCP request indefinitely.

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings that the Switched Rack PDU needs to operate on a network, and other information that affects the operation of the Rack PDU.

The Rack PDU uses the Vendor Specific Information option (option 43) in a DHCP response to determine whether the DHCP response is valid.

Vendor Specific Information (option 43). The Vendor Specific Information option contains up to two APC specific options encapsulated in a Tag/Len/Data format: the APC Cookie and the Boot Mode Transition.

APC Cookie. Tag 1, Len 4, Data “1APC”

Option 43 notifies the Rack PDU that a DHCP server has been configured to service APC devices. By default, the APC Cookie must be present in this DHCP response option before the Rack PDU can accept the lease.



Note

Use the **DHCP Cookie Is** setting described in [Switched Rack PDU settings](#) to disable the APC cookie requirement.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
```

Boot Mode Transition. Tag 2, Len 1, Data 1/2

This option 43 setting enables or disables the **After IP Assignment** option which, by default, causes the **Boot mode** option to use the setting that reflects the server that provided the TCP/IP settings (**DHCP Only** or **BOOTP Only**):

- For a data value of 1, the **After IP Assignment** option is disabled, and the **Boot mode** option remains in its **DHCP & BOOTP** setting after successful network assignment. Whenever the Switched Rack PDU restarts, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.



See [DHCP & BOOTP boot process](#).

- For a data value of 2, the **After IP Assignment** option is enabled and the **Boot mode** option switches to **DHCP Only** when the embedded management card accepts the DHCP response. Whenever the Rack PDU restarts, it will request its network assignment (TCP/IP settings) from a DHCP server only.



For more information about the **After IP Assignment**, see [Switched Rack PDU settings](#).

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie and the disable Boot Mode Transition setting:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43 0x02 0x01 0x01
```

TCP/IP options. The Switched Rack PDU uses the following options within a valid DHCP response to define its TCP/IP settings:

- **IP Address** (from the **yiaddr** field of the DHCP response): Provides the IP address that the DHCP server is leasing to the Rack PDU.
- **Subnet Mask** (option 1): Provides the subnet mask value needed by the Rack PDU to operate on the network.
- **Default Gateway** (option 3): Provides the default gateway address needed by the Rack PDU to operate on the network.
- **Address Lease Time** (option 51): Identifies the length of time for the lease associated with the identified **IP Address**.
- **Renewal Time, T1** (option 58): Identifies how long the Rack PDU must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): Identifies how long the Rack PDU must wait after an IP address lease is assigned before it can seek to rebind that lease.

Miscellaneous options. The Switched Rack PDU uses the following options within a valid DHCP response to define NTP, DNS, hostname, and domain name settings:

- **NTP Server, Primary and Secondary** (option 42): Identifies up to two NTP servers that can be used by the Rack PDU.
- **NTP Time Offset** (option 2): Specifies the offset, in seconds, of the subnet for the Rack PDU from Coordinated Universal Time (UTC).
- **DNS Server, Primary and Secondary** (option 6): Identifies one or two DNS servers that can be used by the Rack PDU.
- **Host Name** (option 12): Identifies the hostname (maximum length of 32 characters) to be used by the Rack PDU.
- **Domain Name** (option 15): Identifies the domain name (maximum length of 64 characters) to be used by the Rack PDU.

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the Switched Rack PDU is subject to the same exposure as other devices on the network.

Use the information in this section to plan and implement the security features appropriate for your environment.

Summary of access methods

Serial control console.

| Security Access | Description |
|--------------------------------------|-----------------|
| Access is by user name and password. | Always enabled. |

Remote control console.

| Security Access | Description |
|---|---|
| Available methods: <ul style="list-style-type: none">• User name and password• Selectable server port• Server Enable/Disable• Secure SHell (SSH) | For high security, use SSH. <ul style="list-style-type: none">• With Telnet, the user name and password are transmitted as plain text.• SSH disables Telnet and provides encrypted access to the control console interface to provide additional protection from attempts to intercept, forge, or alter data during data transmission. |

SNMP.

| Security Access | Description |
|---|---|
| Available methods: <ul style="list-style-type: none">• Community Name• Domain Name• NMS IP filters• Agent Enable/Disable• 4 access communities with read/write/disable capability | The domain name restricts access only to the NMS as that location, and the NMS IP filters allow access only from designated IP addresses. <ul style="list-style-type: none">• 162.245.12.1 allows only the NMS with that IP address to have access.• 162.245.12.255 allows access for any NMS on the 162.245.12 segment.• 162.245.255.255 allows access for any NMS on the 162.245 segment.• 162.255.255.255 allows access for any NMS on the 162 segment.• 0.0.0.0 or 255.255.255.255 allows access for any NMS. |

File transfer protocols.

| Security Access | Description |
|--|---|
| Available methods: <ul style="list-style-type: none">• User name and password• Selectable server port• Server Enable/Disable• Secure CoPy (SCP) | With FTP, the user name and password are transmitted as plain text, and files are transferred without the protection of encryption. Using SCP instead of FTP encrypts the user name and password and the files being transferred, such as firmware updates, configuration files, log files, Secure Sockets Layer (SSL) certificates, and Secure SHell (SSH) host keys. If you choose SCP as your file transfer protocol, enable SSH and disable FTP. |

Web Server.

| Security Access | Description |
|--|---|
| Available methods: <ul style="list-style-type: none">• User name and password• Selectable server port• Server Enable/Disable• Secure Sockets Layer (SSL) and Transport Layer Security (TLS) | <p>In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption).</p> <p>SSL and TLS are available on Web browsers supported for the Switched Rack PDU and on most Web servers. The Web protocol Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.</p> |

RADIUS.

| Security Access | Description |
|--|---|
| Available methods: <ul style="list-style-type: none">• Centralized authentication of access rights• A server secret shared between the RADIUS server and the Rack PDU | <p>RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization and accounting service used to centrally administer remote access for each Rack PDU.</p> |

Changing default user names and passwords immediately

As soon as you complete the installation and initial configuration of the Rack PDU, immediately change the default user names and passwords. Configuring unique user names and passwords is essential to establish basic security for your system.

Port assignments

If a Telnet, FTP, SSH/SCP, or Web/SSL/TLS server uses a non-standard port, a user must specify the port when using the client interface, such as a Web browser. The non-standard port address becomes an extra “password,” hiding the server to provide an additional level of security. The TCP ports for which these servers listen are initially set at the standard “well known ports” for the protocols. To hide the interfaces, use any port numbers from 5000 to 32768.

User names, passwords, community names (SNMP)

All user names, passwords, and community names for SNMP are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log on to the accounts of the control console or Web interface of the Switched Rack PDU. If your network requires the higher security of the encryption-based options available for the control console and Web interface, be sure to disable SNMP access or set its access to read-only. (Read-only access allows you to receive status information and to use SNMP traps.)

Authentication versus Encryption

You can select to use security features for the Switched Rack PDU that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data are not being transferred.

To ensure that data and communication between the Switched Rack PDU and the client interfaces, such as the control console and the Web interface, cannot be intercepted, you can provide a greater level of security by using one or more of the following encryption-based methods:

- For the Web interface, use the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.
- To encrypt user names and passwords for control console access, use the Secure SHell (SSH) protocol.
- To encrypt user names, passwords, and data for the secure transfer of files, use the Secure CoPy (SCP) protocol.



For more information on these protocols for encryption-based security, see [Secure SHell \(SSH\)](#) and [Secure CoPy \(SCP\)](#) and [Secure Sockets Layer \(SSL\)/Transport Layer Security \(TLS\)](#).

Encryption

Secure SHell (SSH) and Secure CoPy (SCP)

The Secure SHell (SSH) protocol provides a secure mechanism to access computer consoles or *shells* remotely. The protocol authenticates the server (in this case, the Switched Rack PDU) and encrypts all transmissions between the SSH client and the server.

- SSH is an alternative to Telnet, which does not provide encryption.
- SSH protects the username and password, the credentials for authentication, from being used by anyone intercepting network traffic.
- To authenticate the SSH server (the Switched Rack PDU) to the SSH client, SSH uses a host key that is unique to the SSH server and that provides an identification that cannot be falsified. Therefore, an invalid server on the network cannot obtain a user name and password from a user by presenting itself as a valid server.



See also

To create a host key, see [Create an SSH Host Key](#).

- The Switched Rack PDU supports versions 1 and 2 of SSH. The encryption mechanisms of the versions differ, and each version has advantages. Version 1 provides faster login to the Rack PDU, and version 2 provides improved protection from attempts to intercept, forge, or change data that are transmitted.
- When you enable SSH, Telnet is automatically disabled.
- The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet.



For information on supported SSH client applications, see [Telnet/SSH](#).

Secure CoPy (SCP) is a secure file transfer application that you can use instead of FTP. SCP uses the SSH protocol as the underlying transport protocol for encryption of user names, passwords, and files.

- When you enable and configure SSH, you automatically enable and configure SCP. No further configuration of SCP is needed.
- You must explicitly disable FTP. It is **not** disabled by enabling SSH.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

For secure Web communication, you enable Secure Sockets Layer (SSL) and Transport Layer Security (TLS) by selecting HTTPS (SSL/TLS) as the protocol mode to use for access to the Web interface of the Switched Rack PDU. Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and pages that are returned by the web server to the user. Originally developed by Netscape, it has become an internet standard supported by most Web browsers.

The Switched Rack PDU supports SSL version 3.0 and TLS version 1.0. Most browsers let you select the version of SSL to enable.



When SSL is enabled, your browser displays the lock icon, usually at the bottom of the screen.

SSL uses a digital certificate to enable the browser to authenticate the server (in this case, the Switched Rack PDU). The browser verifies the following:

- The format of the server certificate is correct.
- The server certificate's expiration date and time has not passed.
- The DNS name or IP address specified when a user logs on matches the common name in the server certificate.
- The server certificate is signed by a trusted certifying authority.

Each major browser manufacturer distributes CA root certificates of the commercial Certificate Authorities in the certificate store (cache) of its browser so that it can compare the signature on the server certificate to the signature on a CA root certificate.

You can use the APC Security Wizard, provided on the APC Rack Power Distribution Unit *Utility* CD that came with your Rack PDU, to create a certificate signing request to an external Certificate Authority, or if you do not want to use an existing Certificate Authority, you can create an APC root certificate to upload to a browser's certificate store (cache). You can also use the Wizard to create a server certificate to upload to the Rack PDU.



See [Creating and Installing Digital Certificates](#) for a summary of how these certificates are used.



See also

To create certificates and certificate requests, see [Create a Root Certificate & Server Certificates](#) and [Create a Server Certificate and Signing Request](#).

SSL also uses various algorithms and encryption ciphers to authenticate the server, encrypt data, and ensure the integrity of the data (i.e., that it has not been intercepted and sent by another server).



See [CipherSuite](#) to select which authentication and encryption algorithms to use.



Note

Web browsers cache (save) Web pages that you recently accessed and allow you to return to those pages without re-entering your user name and password. Always close your browser session before you leave your computer unattended.

Creating and Installing Digital Certificates

Purpose

For network communication that requires a higher level of security than password encryption, the Web interface of the Switched Rack PDU supports the use of digital certificates with the Secure Sockets Layer (SSL) protocol. Digital certificates can authenticate the Switched Rack PDU (the server) to the Web browser (the SSL client).

The sections that follow summarize the three methods of creating, implementing, and using digital certificates. Read these sections to determine the most appropriate method for your system.

- **Method 1: Use the auto-generated default certificate.**
- **Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate.**
- **Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate.**



Note

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

Choosing a method for your system

Using the Secure Sockets Layer (SSL) protocol, you can choose any of the following methods for using digital certificates.

Method 1: Use the auto-generated default certificate. When you enable SSL, you must reboot the Rack PDU. During rebooting, if no server certificate exists on the Rack PDU, the Rack PDU generates a default server certificate that is self-signed but that you cannot configure.

This method has the following advantages and disadvantages:

- **Advantages:**

- Before they are transmitted, the user name and password for Rack PDU access and all data to and from the Rack PDU are encrypted.
- You can use this default server certificate to provide encryption-based security while you are setting up either of the other two digital certificate options, or you can continue to use it for the benefits of encryption that SSL provides.

- **Disadvantages:**

- The Rack PDU takes up to 5 minutes to create this certificate, and the Web interface is not available during that time. (This delay occurs the first time you log on after you enable SSL.)
- This method does not include the browser-based authentication provided by a CA certificate (a certificate signed by a Certificate Authority) as Methods 2 and 3 provide. There is no CA Certificate cached in the browser. Therefore, whenever you log on to the Rack PDU, the browser generates a security alert, indicating that a certificate signed by a trusted authority is not available and asking if you want to proceed.
- The default server certificate on the Rack PDU has the Rack PDU's serial number in place of a valid *common name* (the DNS name or the IP address of the Rack PDU). Therefore, although the Rack

PDU can control access to its Web interface by user name, password, and account type (e.g., **Administrator**, **Device Manager**, or **Read Only User**), the browser cannot authenticate what Rack PDU is sending or receiving data.

- The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is only 768 bits. (The public key used in Methods 2 and 3 is 1024 bits, providing more complex encryption and consequently a higher level of security.)

Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate. You use the APC Security Wizard to create two digital certificates:

- A *CA root certificate* (Certificate Authority root certificate) that the APC Security Wizard uses to sign all server certificates and which you then install into the certificate store (cache) of the browser of each user who needs access to the Rack PDU.
- A *server certificate* that you upload to the Rack PDU. When the APC Security Wizard creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the Rack PDU sending or requesting data:

- To identify the Rack PDU, the browser uses the *common name* (IP address or DNS name of the Rack PDU) that was specified in the server certificate's *distinguished name* when the certificate was created.
- To confirm that the server certificate is signed by a “trusted” signing authority, the browser compares the signature of the server certificate with the signature in the root certificate cached in the browser. An expiration date confirms whether the server certificate is current.

This method has the following advantages and disadvantages.

- **Advantages:**
 - Before they are transmitted, the user name and password for Rack PDU access and all data to and from the Rack PDU are encrypted.
 - The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security than the public key used in Method 1. (This longer encryption key is also used in Method 3.)

- The server certificate that you upload to the Rack PDU enables SSL to authenticate that data are being received from and sent to the correct Rack PDU. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
- The root certificate that you install to the browser enables the browser to authenticate the Rack PDU's server certificate to provide additional protection from unauthorized access.
- **Disadvantage:**

Because the certificates do not have the digital signature of a commercial Certificate Authority, you must load a root certificate individually into the certificate store (cache) of each user's browser. (Browser manufacturers already provide root certificates for commercial Certificate Authorities in the certificate store within the browser. See Method 3.)

Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate. Use the APC Security Wizard to create a request (a **.csr** file) to send to a Certificate Authority. The Certificate Authority returns a signed certificate (a **.crt** file) based on information you submitted in your request. You then use the APC Security Wizard to create a server certificate (a **.p15** file) that includes the signature from the root certificate returned by the Certificate Authority. Upload the server certificate to the Rack PDU.



Note

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

This method has the following advantages and disadvantages.

- **Advantages:**

- Before they are transmitted, the user name and password for Rack PDU access and all data to and from the Rack PDU are encrypted.
- You have the benefit of authentication by a Certificate Authority that already has a signed root certificate in the certificate cache of the browser. (The CA certificates of commercial Certificate Authorities are distributed as part of the browser software, and a Certificate Authority of your own company or agency has probably already loaded its CA certificate to the browser store of each user's browser.) Therefore, you do not have to upload a root certificate to the browser of each user who needs access to the Rack PDU.
- The length of the *public key* (RSA key) that is used for setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security than the public key used in Method 1. (This longer encryption key is also used in Method 2.)

- The server certificate that you upload to the Rack PDU enables SSL to authenticate that data are being received from and sent to the correct Rack PDU. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
- The browser matches the digital signature on the server certificate that you uploaded to the Rack PDU with the signature on the CA root certificate that is already in the browser's certificate cache to provide additional protection from unauthorized access.
- **Disadvantages:**
 - Setup requires the extra step of requesting a signed root certificate from a Certificate Authority.
 - An external Certificate Authority may charge a fee for providing signed certificates.

Firewalls

Although some methods of authentication provide a higher level of security than others, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Using the APC Security Wizard

Overview

Authentication

Authentication verifies the identity of a user or a network device (such as an APC Switched Rack PDU). Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the Switched Rack PDU supports more secure methods of authentication.

- Secure Sockets Layer (SSL), used for secure Web access, uses digital certificates for authentication. A digital *CA root* certificate is issued by a Certificate Authority (CA) as part of a public key infrastructure, and its digital signature must match the digital signature on a server certificate on the Rack PDU.
- Secure SHell (SSH), used for remote terminal access to the Rack PDU's control console, uses a public *host key* for authentication rather than a digital certificate.

How certificates are used. Most Web browsers, including all browsers supported by the Switched Rack PDU, contain a set of CA root certificates from all of the commercial Certificate Authorities.

Authentication of the server (in this case, the Rack PDU) occurs each time a connection is made from the browser to the server. The browser checks to be sure that the server's certificate is signed by a Certificate Authority known to the browser. For this authentication to occur:

- Each Switched Rack PDU with SSL enabled must have a server certificate on the Rack PDU itself.
- Any browser that is used to access the Rack PDU's Web interface must contain the CA root certificate that signed the server certificate.

If authentication fails, the browser prompts you on whether to continue despite the fact that it cannot authenticate the server.

If your network does not require the authentication provided by digital certificates, you can use the default certificate that the Rack PDU generates automatically. The default certificate's digital signature will not be recognized by browsers, but a default certificate enables you to use SSL for the encryption of transmitted user names, passwords, and data. (If you use the default certificate, the browser prompts you to agree to unauthenticated access before it logs you on to the Web interface of the Rack PDU.)

How SSH host keys are used. An SSH *host key* authenticates the identity of the server (the Switched Rack PDU) each time an SSH client contacts the Rack PDU. Each Switched Rack PDU with SSH enabled must have an SSH host key on the Rack PDU itself.

Files you create for SSL and SSH security

Use the APC Security Wizard to create the following components of an SSL and SSH security system:

- The server certificate for the Switched Rack PDU, if you want the benefits of authentication that such a certificate provides. You can create either of the following types of server certificate:

- A server certificate signed by a custom CA root certificate also created with the APC Security Wizard. Use this method if your company or agency does not have its own Certificate Authority and you do not want to use an external Certificate Authority to sign the server certificate.
- A server certificate signed by an external Certificate Authority. This Certificate Authority can be one that is managed by your own company or agency or can be one of the commercial Certificate Authorities whose CA root certificates are distributed as part of a browser's software.
- A certificate signing request containing all the information required for a server certificate except the digital signature. You need this request if you are using an external Certificate Authority.
- A CA root certificate.
- An SSH host key that your SSH client program uses to authenticate the Rack PDU when you log on to the control console interface.



Note

All public keys for SSL certificates and all host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys. If you do not create and use SSL server certificates and SSH host keys with the APC Security Wizard, the Rack PDU generates 768-bit RSA keys.

Only APC server management and key management products can use server certificates, host keys, and CA root certificates created by the APC Security Wizard. These files will not work with products such as OpenSSL® and Microsoft IIS.

Create a Root Certificate & Server Certificates

Summary

Use this procedure if your company or agency does not have its own Certificate Authority and you do not want to use a commercial Certificate Authority to sign your server certificates.



Note

The public RSA key that is part of a certificate generated by the APC Security Wizard is 1024 bits. (The default key generated by the Rack PDU, if you do not use the Wizard, is 768 bits.)

- Create a CA root certificate that will be used to sign all server certificates to be used with Switched Rack PDUs. During this task, two files are created.
 - The file with the **.p15** extension is an encrypted file which contains the Certificate Authority's private key and public root certificate. This file signs the server certificates.
 - The file with the **.crt** extension, which contains only the Certificate Authority's public root certificate. You load this file into each Web browser that will be used to access the Switched Rack PDU so that the browser can validate the server certificate of the Rack PDU.
- Create a server certificate, which is stored in a file with a **.p15** extension. During this task, you are prompted for the CA root certificate that signs the server certificate.
- Load the server certificate onto the Switched Rack PDU.
- For each Switched Rack PDU that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the CA root certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Rack PDU *Utility* CD that came with your Rack PDU.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled “Step 1,” select **CA Root Certificate** as the type of file to create.
4. Enter a name for the file that will contain the Certificate Authority’s public root certificate and private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled “Step 2,” provide the information to configure the CA root certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter an identifying name of your company or agency; use only alphanumeric characters, with no spaces.



Note

By default, a CA root certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate’s unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.



Note

The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate has been created and instructs you on the next tasks.
 - This screen displays the location and name of the **.p15** file that you will use to sign the server certificates.
 - This screen also displays the location and name of the **.crt** file, which is the CA root certificate that you will load into the browser of each user who needs to access the Rack PDU.

Load the CA root certificate to your browser. Load the **.crt** file to the browser of each user who needs to access the Rack PDU.



See also See the help system of the browser for information on how to load the **.crt** file into the browser's certificate store (cache). Following is a summary of the procedure for Microsoft Internet Explorer.

1. Select **Tools**, then **Internet Options** from the menu bar.
2. On the **Content** tab in the **Internet Options** dialog box, click **Certificates** and then **Import**.
3. The Certificate Import Wizard will guide you through the rest of the procedure. The file type to select is X.509, and the CA Public Root Certificate is the **.crt** file created in the procedure **Create a Root Certificate & Server Certificates**.

Create an SSL Server User Certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **SSL Server Certificate** as the type of file to create.
3. Enter a name for the file that will contain the server certificate and the private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
4. Click the **Browse** button, and select the CA root certificate created in the procedure **Create a Root Certificate & Server Certificates**. The CA Root Certificate is used to sign the Server User Certificate being generated.
5. On the screen labeled Step 2, provide the information to configure the server certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP address or DNS name of the server (Switched Rack PDU). Because the configuration information is part of the signature, it cannot be exactly the same as the information you provided when creating the CA root certificate; the information you provide in some of the fields must be different.



Note

By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.



Note

The information for every certificate must be unique. The configuration of a server certificate cannot be the same as the configuration of the CA root certificate. (The expiration date is not considered part of the unique configuration; some other configuration information must also differ.)

7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the Switched Rack PDU. It displays the location and name of the Server Certificate, which has a **.p15** file extension and contains the Rack PDU private key and public root certificate.

Load the server certificate to the Rack PDU. Perform these steps:

1. On the **Network** menu of the Web interface of the Switched Rack PDU, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure **Create a Root Certificate & Server Certificates**. (The default is **C:\Program Files\American Power Conversion\APC Security Wizard.**)



Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Rack PDU. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Rack PDU. For SCP, the command to transfer a certificate named **cert.p15** to a Rack PDU with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```


Create a Server Certificate and Signing Request

Summary

Use this procedure if your company or agency has its own Certificate Authority or if you plan to use a commercial Certificate Authority to sign your server certificates.

- Create a Certificate Signing Request (CSR). The CSR contains all the information for a server certificate except the digital signature. This process creates two output files:
 - The file with the **.p15** extension contains the Switched Rack PDU's private key.
 - The file with the **.csr** extension contains the certificate signing request, which you send to an external Certificate Authority.
- When you receive the signed certificate from the Certificate Authority, import that certificate. Importing the certificate combines the **.p15** file containing the private key and the file containing the signed certificate from the external Certificate Authority. The output file is a new encrypted server certificate file with a **.p15** extension.
- Load the server certificate onto the Switched Rack PDU.
- For each Switched Rack PDU that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the Certificate Signing Request (CSR). Perform these steps.

(Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Rack PDU *Utility* CD that came with your Rack PDU.

2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled “Step 1,” select **Certificate Request** as the type of file to create.
4. Enter a name for the file that will contain the Switched Rack PDU's private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled Step 2, provide the information to configure the certificate signing request (CSR) with the information that you want the signed server certificate to contain. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP Address or DNS name of the Switched Rack PDU.



By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.



The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate signing request has been created and displays the location and name of the file, which has a **.csr** extension.

8. Send the certificate signing request to an external Certificate Authority, either a commercial Certificate Authority or, if applicable, a Certificate Authority managed by your own company or agency.



See also

See the instructions provided by the Certificate Authority regarding the signing and issuing of server certificates.

Import the signed certificate. When the external Certificate Authority returns the signed certificate, perform these steps to import the certificate. This procedure combines the signed certificate and the private key into an SSL server certificate that you then upload to the Switched Rack PDU. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **Import Signed Certificate**.
3. Browse to and select the signed server certificate that you received from the external Certificate Authority. The file has a **.cer** or **.crt** extension.
4. Browse to and select the file you created in step 4 of the task, **Create the Certificate Signing Request (CSR)**. This file has a **.p15** extension, contains the Switched Rack PDU's private key, and, by default, is located in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Specify a name for the output file that will be the signed server certificate that you upload to the Rack PDU. The file must have a **.p15** extension.
6. Click **Next** to generate the server certificate. The certificate's **Issuer Information** on the summary screen confirms that the external Certificate Authority signed the certificate.

7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the Switched Rack PDU. It displays the location and name of the server certificate, which has a **.p15** file extension and contains the Rack PDU's private key and the public key obtained from the **.cer** or **.crt** file.

Load the server certificate to the Rack PDU. Perform these steps:

1. On the **Network** menu of the Web interface of the Switched Rack PDU, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure **Import the signed certificate**. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard**.)



Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Rack PDU. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Rack PDU. For SCP, the command to transfer a certificate named **cert.p15** to a Rack PDU with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```

Create an SSH Host Key

Summary

This procedure is optional. If you select SSH encryption, but do not create a host key, the Switched Rack PDU generates a 768-bit RSA key when it reboots. Host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys.

- Use the APC Security Wizard to create a host key, which is encrypted and stored in a file with **.p15** extension.
- Load the host key onto the Rack PDU.

The procedure

Create the host key. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Rack PDU *Utility* CD that came with your Rack PDU.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled Step 1, select **SSH Server Host Key** as the type of file to create.
4. Enter a name for the file that will contain the host key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Click **Next** to generate the Host Key.
6. The summary screen displays the SSH version 1 and version 2 fingerprints, which are unique for each host key and identify the host key. After you load the host key onto the Rack PDU, you can verify that

the correct host key was uploaded by verifying that the fingerprints displayed here match the SSH fingerprints on the Rack PDU, as displayed by your SSH client program.

7. The last screen verifies that the host key has been created and instructs you on the next task, to load the host key to the Switched Rack PDU. It displays the location and name of the host key, which has a **.p15** file extension.

Load the host key to the Rack PDU. Perform these steps:

1. On the **Network** menu of the Web interface of the Switched Rack PDU, select the **Telnet/SSH** option.
2. In the **SSH User Host Key File** section of the page, browse to the host key, the **.p15** file you created in the procedure **Create the host key**. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard**.)
3. On the **SSH Host Key Fingerprint** section of the page, note the fingerprint for the version (or versions) of SSH you are using. Then log on to the Rack PDU through your SSH client program, and verify that the correct host key was uploaded by verifying that these fingerprints match the fingerprints that the client program displays.



Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the Rack PDU. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Rack PDU. For SCP, the command to transfer a host key named **hostkey.p15** to a Rack PDU with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\hostkey.p15
```

APC Device IP Configuration Wizard

Purpose and Requirements

Purpose: configure basic TCP/IP settings

You can use the APC Device IP Configuration Wizard to configure the basic TCP/IP settings (IP address, subnet mask, and default gateway) of the following:

- Network Management Cards
- Devices that contain embedded Network Management Cards

Using the Wizard, you can configure the basic TCP/IP settings of installed or embedded Network Management Cards in either of the following ways:

- Automatically discover and configure unconfigured Network Management Cards remotely over your TCP/IP network.
- Configure or reconfigure a Network Management Card through a direct connection from the serial port of your computer to the device that contains the card.



Note

The Wizard can discover and configure Network Management Cards only if they are on the same network segment as the computer that is running the Wizard.

System requirements

The Wizard runs on Windows NT[®], Windows 2000, Windows 2003, and Windows XP Intel-based workstations.

Install the Wizard

Automated installation

If autorun is enabled on your CD-ROM drive, the installation program starts automatically when you insert the CD.

Manual installation

If autorun is not enabled on your CD-ROM drive, run **setup.exe** in the Wizard directory on the CD, and follow the on-screen instructions.

You can also download the latest version of the APC Device IP Configuration Wizard from the APC Web site, www.apc.com and run **setup.exe** from the folder to which you downloaded it.

Use the Wizard

Launch the Wizard

The installation creates a shortcut link in the **Start** menu that you can use to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard, be sure that you have the information you will need during the configuration procedure:

1. Contact your network administrator to obtain valid TCP/IP settings to use.
2. If you are configuring multiple unconfigured Network Management Cards, obtain the MAC address of each one so that you can identify each Network Management Card that the Wizard discovers. (The Wizard displays the MAC address for a discovered card on the same screen on which you then enter the TCP/IP settings.)
 - For Network Management Cards that you install, the MAC address is on a label on the bottom of the card.
 - For embedded Network Management Cards, the MAC address is on a label on the device containing the card — for example, usually on the side of a device that you mount in a rack.

You can also obtain the MAC address from the Quality Assurance slip that came with the Network Management Card or with the device containing an embedded Network Management Card.

Run the Wizard to perform the configuration. To discover and configure, over the network, installed or embedded Network Management Cards that are not configured:

1. From the **Start** menu, launch the Wizard. The Wizard automatically detects the first Network Management Card that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the unconfigured Network Management Card identified by the MAC address at the top of the screen. Then click **Next >**.
4. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
5. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
6. The Wizard searches for another installed or embedded but unconfigured Network Management Card. If it finds one, it displays the screen with data entry boxes for the TCP/IP settings of that card.
 - To skip configuring the card whose MAC address is currently displayed, click **Cancel**.
 - To configure the TCP/IP settings of the next card, repeat this procedure beginning at step 4.

Configure or reconfigure the TCP/IP settings locally

To configure a single Network Management Card through a serial connection:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the serial configuration cable that came with the Network Management Card or with the device that contains an embedded Network Management Card.
 - a. Connect one end to an available communications port on your computer. Make sure no other application is using the port.
 - b. Connect the other end to the serial port of the card or device.
3. From the **Start** menu, launch the Wizard application.
 - If the Network Management Card is not configured, wait until it is detected by the Wizard.
 - If you are assigning basic TCP/IP settings serially to a Network Management Card, click **Next >** to move to the next screen.
4. Select **Locally (through the serial port)**, and click **Next >**.
5. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the Network Management Card. Then click **Next >**.
6. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
7. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
8. If you selected **Start a Web browser when finished** in step 6, you can now configure other parameters through the Web interface of the card or device.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

As an Administrator, you can retrieve a dynamically generated .ini file of a Switched Rack PDU's current configuration and export that file to another Switched Rack PDU or to multiple Switched Rack PDUs.

1. Configure a Switched Rack PDU to have the settings you want to export.
2. Retrieve the .ini file from that Rack PDU.
3. Customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. Use any of the file transfer protocols supported by the Switched Rack PDU to transfer the copied file to one or more additional Rack PDUs. (To transfer the file to multiple Rack PDUs simultaneously, write an FTP or SCP script that repeats the steps for transferring the file to a single Rack PDU.)
5. Each receiving Switched Rack PDU stores the file temporarily in its flash memory, uses it to reconfigure its own Rack PDU settings, and then deletes the file.

Contents of the .ini file

The config.ini file that you retrieve from a Switched Rack PDU contains the following:

- *section headings*, which are category names enclosed in brackets ([]), and under each section heading, *keywords*, which are labels describing specific Rack PDU settings.



Note

Only section headings and keywords supported for the specific device associated with the Rack PDU from which you retrieve the file are included.

- Each keyword is followed by an equals sign and the current *value* for that parameter's setting, either the default value (if the value has not been specifically configured) or the configured value.
 - The `Override` keyword, with its default value, prevents one or more keywords and their device-specific values from being exported. In the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Rack PDU) blocks the exporting of the values for the keywords `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.
 - You must edit the section `[SystemDate/Time]` if you want to set the system date and time of a receiving Rack PDU or cause that Rack PDU to use an NTP Server to set its date and time.



See [Customizing](#) for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one Switched Rack PDU and export them to one or more other Switched Rack PDUs.

Retrieving. To set up and retrieve an .ini file to export:

1. Configure a Rack PDU with the settings you want to export.



Note

To avoid errors, configure the Rack PDU by using its Web interface or control console whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the file config.ini from the Rack PDU you configured:
 - a. Open a connection to the Rack PDU, using its IP Address. For example:

```
ftp> open 158.165.2.132
```

- b. Log on, using the Administrator user name and password configured for the Rack PDU.
- c. Retrieve the config.ini file containing the Rack PDU's current settings:

```
ftp> get config.ini
```

The file is written to the folder from which you launched FTP.



See also

To create batch files and use an APC utility to retrieve configuration settings from multiple Rack PDUs and export them to other Rack PDUs, see *Release Notes: ini File Utility, version 1.0* ([.\doc\en\ininotes.pdf](#)) on the APC Rack PDU *Utility* CD that came with your Rack PDU.

Customizing. You must customize the file to change at least the TCP/IP settings before you export it.

1. Use a text editor to customize the file.
 - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
 - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=" "` indicates that the URL is intentionally undefined.
 - To define values, opening and closing quotation marks are optional, except to enclose values that contain leading or trailing spaces or values which are already enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)
 - To export a specific system date and time or any scheduled events, you must configure the values directly in the .ini file.
 - To export a specific system time, export only the configured `[SystemDate/Time]` section as a separate .ini file. (The time necessary to export a large file would cause the configured time to be significantly inaccurate.)
 - For greater accuracy, if the Switched Rack PDUs receiving the file can access a Network Time Protocol (NTP) Server, set the value for the `NTPEnable` keyword as follows:

```
NTPEnable=enabled
```
 - Add comments about changes that you made. The first printable character of a comment line must be a semicolon (;).
2. Copy the customized file to another file name in the same folder:
 - The copy, which you will export to other Rack PDUs, can have any file name up to 64 characters and must have the .ini file suffix.
 - Retain the original customized file for future use. **The file that you retain is the only record of your comments.** They are removed automatically from the file that you export.

Exporting the file to a single Rack PDU. To export the .ini file to another Switched Rack PDU, use any of the file transfer protocols supported by Switched Rack PDUs (including FTP, FTP Client, SCP, and TFTP). The following example uses FTP:

1. From the folder containing the customized .ini file and its copy, use FTP to log in to the Rack PDU to which you are exporting the .ini file. For example:

```
ftp> open 158.165.4.135
```

2. Export the copy of the customized .ini file. The receiving Rack PDU accepts any file name that has the .ini suffix, is no more than 64 characters in length, and is exported to its root directory.

```
ftp> put filename.ini
```

Exporting the file to multiple Rack PDUs. To export the .ini file to multiple Switched Rack PDUs:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Management Card.
- Use a batch processing file and the APC .ini file utility.



To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* (`.\doc\en\ininotes.pdf`) on the APC Rack PDU *Utility* CD that came with your Rack PDU.

See also

The Upload Event and Error Messages

The event and its error messages

The following system event occurs when the receiving Switched Rack PDU completes using the .ini file to update its settings.

Configuration file upload complete, with *number* valid values

This event has no default severity level.

If a keyword, section name, or value is invalid, the event text is extended to include notification of the following errors.



Note

The export to and the subsequent upload by the receiving Rack PDU succeeds even if there are errors.

| Event text | Description |
|--|---|
| Configuration file warning: Invalid keyword on line <i>number</i> . Configuration file warning: Invalid value on line <i>number</i> . | A line with an invalid keyword or value is ignored. |
| Configuration file warning: Invalid section on line <i>number</i> . | If a section name is invalid, all keyword/value pairs in that section are ignored. |
| Configuration file warning: Keyword found outside of a section on line <i>number</i> . | A keyword entered at the beginning of the file (i.e., before any section headings) is ignored. |
| Configuration file warning: Configuration file exceeds maximum size. | If the file is too large, the Rack PDU stores and processes what it can, but ignores what it cannot. Reduce the size of the file, or divide it into two files, and try uploading again. |

Messages in config.ini

A feature might not be supported for the device from which you retrieve the configuration settings or might not be supported for the device to which you export the configuration settings. In this case, the user configuration file contains, under the section name for that feature, a message stating that the feature is not supported. No keywords and values are listed, and that feature will not be configured on any device to which you export the user configuration file.

Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values.



See [Contents of the .ini file](#) for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other Rack PDUs. Therefore, you can ignore these error messages. To prevent these error messages from occurring, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Using the APC Device IP Configuration Wizard

On Windows operating systems, instead of using the preceding procedure for exporting .ini files, you can choose to update the basic TCP/IP settings of Rack PDUs by using the APC Device IP Configuration Wizard.



See [APC Device IP Configuration Wizard](#) for a detailed description of how to discover and configure unconfigured Switched Rack PDUs remotely over your TCP/IP network or configure or reconfigure a Switched Rack PDU through a direct connection from the serial port of your computer to the Switched Rack PDU.

File Transfers

Introduction

Overview

The Switched Rack PDU automatically recognizes binary firmware files. Each of these files contains a header and one or more Cyclical Redundancy Checks (CRCs) to ensure that the data contained in the file is not corrupted before or during the transfer operation.

When new firmware is transmitted to the Rack PDU, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to Switched Rack PDUs.



To transfer a firmware file to a Rack PDU, see [Upgrading Firmware: Methods and Tools](#).

To verify a file transfer, see [Verifying Upgrades and Updates](#).

Upgrading Firmware: Methods and Tools

Benefits of upgrading firmware

Upgrading the firmware on the Switched Rack PDU has the following benefits:

- New firmware has the latest bug fixes and performance improvements.
- New features become available for immediate use.
- Keeping the firmware versions consistent across your network ensures that all Switched Rack PDUs support the same features in the same manner.

Firmware files (Switched Rack PDU)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module.

The APC Operating System (AOS) and application module files used with the Switched Rack PDU share the same basic format:

```
apc_hw0x_type_version.bin
```

- `apc`: Indicates that this is an APC file.
- `hw0x`: Identifies the version of the Switched Rack PDU that will run this binary file.
- `type`: Identifies whether the file is for the APC Operating System (AOS) or the application module (APP) for the Switched Rack PDU.
- `version`: The version number of the application file. For example, a code of 266 would indicate version 2.6.6.
- `bin`: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An automated self-extracting executable tool combines the firmware modules that you need to automate your upgrades on any supported Windows operating system

- The version of the tool on the APC Rack PDU *Utility* CD that came with your Rack PDU will upgrade your device to the latest AOS and application modules available when the CD was released.
- If a later firmware upgrade is available, you can obtain an updated version of the tool at no cost from the support section of the APC web site www.apc.com/tools/download. At this Web page, find the latest firmware release for your APC product (in this case, your Rack PDU) and download the automated tool, not the individual firmware modules.

If the AOS firmware module you already have is a 1.x.x version, the executable tool must perform two consecutive upgrades:

- The first upgrade is from version 1.x.x to the latest available 2.0.x version of the AOS firmware module.
- The second upgrade is from the 2.0.x version to the most recently released version of the AOS module.

The tool therefore contains firmware modules for both upgrades.

Each upgrade tool is specific to an APC product type. Do not use the tool from one product CD to upgrade firmware of a different APC product. If you use a version of the tool from the APC Web site, make sure that you use the upgrade tool that corresponds with your APC product type.

Manual upgrades, primarily for Linux systems. If all computers on your network are running Linux, you must upgrade the firmware of your Rack PDUs manually, i.e., by using the separate APC firmware modules (AOS module and application module).



If you have a networked computer running a supported Microsoft Windows operating system on your network, you can use the tool described in [Automated upgrade tool for Microsoft Windows systems](#) to upgrade the firmware of a Switched Rack PDU automatically over the network. This tool automates the entire upgrade process, even if your current firmware is a 1.x.x version.



Note

When performing a manual upgrade, not using the automated tool, you cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.x.x to firmware version 2.1.0 or later. The upgrade attempt will fail. You must first upgrade to the latest available 2.0.x version of the AOS module and then to the later version.

You can obtain the individual firmware modules you need for a manual firmware upgrade from the support section of the APC Web site www.apc.com/tools/download.

Firmware file transfer methods

To upgrade the firmware of a Switched Rack PDU:

- From a networked computer running a Microsoft Windows operating system, you can use the automated firmware upgrade tool on your CD or downloaded from the APC Web site.
- From a networked computer on any supported operating system, you can use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a Switched Rack PDU that is not on your network, you can use XMODEM through a serial connection to transfer the individual AOS and application firmware modules from your computer to the Switched Rack PDU.



Note

When you transfer individual firmware modules and do not use the automated firmware upgrade tool to upgrade the firmware for a Rack PDU, you must transfer the APC Operating System (AOS) module to the Rack PDU before you transfer the application module.



For more information about the firmware modules, see [Firmware files \(Switched Rack PDU\)](#).

Use FTP or SCP to upgrade one Rack PDU

Instructions for using FTP. For you to be able to use FTP to upgrade a single Switched Rack PDU over the network:

- The Switched Rack PDU must be connected to the network.
- The FTP server must be enabled at the Switched Rack PDU.
- The Switched Rack PDU must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

To use FTP to upgrade the Rack PDU:

1. Open an MS-DOS command prompt window on a computer that is connected to the network. Go to the directory that contains the firmware upgrade files, and list the files. For the directory `C:\apc`, the commands would be those shown in **bold**:

```
C:\>cd\apc
```

```
C:\apc>dir
```

Files listed for a Switched Rack PDU, for example, might be the following:

```
- apc_hw02_aos_264.bin
```

```
- apc_hw02_app_266.bin
```

2. Open an FTP client session:

```
C:\apc>ftp
```

3. Type `open` and the Switched Rack PDU's IP address, and press ENTER. If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default of **21**, you must use the non-default value in the FTP command.
 - a. For some FTP clients, use a colon to add the port number to the end of the IP address.
 - b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the Rack PDU's **FTP Server Port** setting has been changed from its default of **21**, such as to

21000, you would use the following command for a Windows FTP client transferring a file to a Rack PDU with an IP address of 150.250.6.10.

```
ftp> open 150.250.6.10 21000
```

4. Log on using the Administrator user name and password. (**apc** is the default for both.)
5. Upgrade the AOS. For example:

```
ftp> bin  
ftp> put apc_hw02_aos_264.bin
```
6. When FTP confirms the transfer, type `Quit` to close the session.
7. Wait 20 seconds, and then repeat step 2 through step 6, but in step 5, use the application module file name instead of the AOS module.

Instructions for using SCP. To use Secure CoPy (SCP) to upgrade the firmware for one Rack PDU:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Rack PDU. The following example assumes a Rack PDU IP address of 158.205.6.185, and an AOS module of **apc_hw02_aos_264.bin**.

```
scp apc_hw02_aos_264.bin apc@158.205.6.185:apc_hw02_aos_264.bin
```
3. Use a similar SCP command line, with the name of the application module instead of the AOS module, to transfer the application module to the Rack PDU.

How to upgrade multiple Rack PDUs

Export configuration settings. You can create batch files and use an APC utility to retrieve configuration settings from multiple Rack PDUs and export them to other Rack PDUs.



See *Release Notes: ini File Utility, version 1.0* ([.\doc\en\ininotes.pdf](#)) on the APC Rack PDU *Utility* CD that came with your Rack PDU.

Use FTP or SCP to upgrade multiple Rack PDUs. To upgrade multiple Switched Rack PDUs using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in [Use FTP or SCP to upgrade one Rack PDU](#).

Use XMODEM to upgrade one Rack PDU



Note

You cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.x.x to 2.1.0 or later. The upgrade attempt will fail.

To upgrade the AOS firmware module of an APC device from version 1.x.x to 2.1.0 or later, first upgrade the module to the latest available version 2.0.x AOS firmware module. Then upgrade it again, this time from version 2.0.x to the 2.x.x version you want.

If your APC device is running a 2.0.x of the AOS firmware module already, you can upgrade directly to version 2.1.0 or a later version.

To use XMODEM to upgrade the firmware for a single Switched Rack PDU that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from the support section of the APC web site www.apc.com/tools/download.

2. Select a serial port at the local computer and disable any service which uses that port.
3. Connect the smart-signaling cable that came with the Rack PDU to the selected port and to the serial port at the Rack PDU.
4. Run a terminal program (such as HyperTerminal), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
5. Press ENTER to display the **User Name** prompt.
6. Enter your Administrator user name and password. The default for both is **apc**.
7. Start an XMODEM transfer:
 - a. Select option 3—**System**
 - b. Select option 4—**File Transfer**
 - c. Select option 2—**XMODEM**
 - d. Type `Yes` at the prompt to continue with the transfer.
8. Select the appropriate baud rate. A higher baud rate causes faster firmware upgrades. Also, change the terminal program's baud rate to match the one you selected, and press ENTER.
9. From the terminal program's menu, select the binary AOS file to transfer via XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The Rack PDU will automatically restart.
10. Repeat **step 3** through **step 8** to install the application module. In **step 8**, substitute the application module file name for the AOS module file name.



For information about the format used for application modules, see [Firmware files \(Switched Rack PDU\)](#).

Verifying Upgrades and Updates

Overview

To verify that the firmware upgrade was successful, see the **Last Transfer Result** message, available through the **FTP Server** option of the **Network** menu (in the control console only), or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

| Code | Description |
|----------------------|---|
| Successful | The file transfer was successful. |
| Result not available | There are no recorded file transfers. |
| Failure unknown | The last file transfer failed for an unknown reason. |
| Server inaccessible | The TFTP or FTP server could not be found on the network. |
| Server access denied | The TFTP or FTP server denied access. |
| File not found | The TFTP or FTP server could not locate the requested file. |
| File type unknown | The file was downloaded but the contents were not recognized. |
| File corrupt | The file was downloaded but at least one CRC was bad. |

You can also verify the versions of the upgraded APC Operating System (AOS) and application modules by using the **About System** option in the **System** menu of the control console or in the **Help** menu of the Web interface, or by using an SNMP GET to the MIB II **sysDescr** OID.

Product Information

Warranty and Service

Limited warranty

APC warrants the Switched Rack PDU to be free from defects in materials and workmanship for a period of two years from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment that has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser.

Warranty limitations

Except as provided herein, APC makes no warranties, expressed or implied, including warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

Except as provided above, in no event will APC be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of this product, even if advised of the possibility of such damage.

Specifically, APC is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise. This warranty gives you specific legal rights and you may also have other rights, which vary according to jurisdiction.

Obtaining service

To obtain support for problems with your Switched Rack PDU:

1. Note the serial number and date of purchase. For the serial number, see the **About System** menu option or the label on the bottom of the unit.
2. Contact Customer Support at a phone number located at the end of this manual. A technician will try to help you solve the problem by phone.
3. If you must return the product, the technician will give you a return material authorization (RMA) number. If the warranty expired, you will be charged for repair or replacement.
4. Pack the unit carefully. The warranty does not cover damage sustained in transit. Enclose a letter with your name, address, RMA number and daytime phone number; a copy of the sales receipt; and a check as payment, if applicable.
5. Mark the RMA number clearly on the outside of the shipping carton.
6. Ship by insured, prepaid carrier to the address provided by the Customer Support technician.

Life-Support Policy

General policy

American Power Conversion (APC) does not recommend the use of any of its products in the following situations:

- In life-support applications where failure or malfunction of the APC product can be reasonably expected to cause failure of the life-support device or to affect significantly its safety or effectiveness.
- In direct patient care.

APC will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to APC that (a) the risks of injury or damage have been minimized, (b) the customer assumes all such risks, and (c) the liability of American Power Conversion is adequately protected under the circumstances.

Examples of life-support devices

The term *life-support device* includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief, or other purposes), autotransfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults and infants), anesthesia ventilators, infusion pumps, and any other devices designated as “critical” by the U.S. FDA.

Hospital-grade wiring devices and leakage current protection may be ordered as options on many APC UPS systems. APC does not claim that units with these modifications are certified or listed as hospital-grade by APC or any other organization. Therefore these units do not meet the requirements for use in direct patient care.

Index

A

- About System 31
- Access
 - FTP Server 77
 - limiting NMS SNMP access by IP address 85
 - security options for each interface 117
- Access setting for RADIUS 102
- Access Type setting 85
- Actions 60
- Advanced settings
 - Client ID 75, 112
 - Domain Name 74, 112
 - Ethernet Port Speed 112
 - Host Name 74, 112
 - On Retry Failure 76
 - Port Speed 75
 - Retry Then Fail 75
 - User Class 75, 112
 - Vendor Class 75, 112
- APC Cookie 114
- APC OS 31
- Apply Local Computer Time 105
- Authentication
 - SNMP Traps 63
 - with SSL 124
- Auto Logout 98

B

- Boot mode 110
- Boot mode settings
 - BOOTP only 74
 - DHCP & BOOTP 74
 - DHCP only 74
 - Manual 74

BOOTP

- After IP Assignment setting 112
- Boot mode settings 74
- BOOTP Only boot mode setting 74
- communication settings 75
- DHCP & BOOTP boot process 111
- Remain in DHCP & BOOTP mode setting 112
- Status LED indicating BOOTP requests 13

Browsers

- CA certificates in browser's store (cache) 124
- supported Web browsers 25

C

Certificates

- choosing which method to use 126
- creating and installing for SSL 126
- methods
 - APC Security Wizard creates all certificates 129
 - Use a Certificate Authority (CA) 131
 - Use the APC default certificate 127

CipherSuite

- Choosing SSL encryption ciphers and hash algorithms 92
- purpose of the algorithms and ciphers 125

Client ID setting 75, 112

Community Name 63
setting 84

config.ini file, contents 154

Configuring

SSL/TLS 88

Control console

Device Manager menu 22

- navigating menus 21
- refreshing menus 21
- Cookie
 - APC 114
- Customizing user configuration files 156

D

- Data log
 - configuration 70
 - Log Interval setting 70
 - using FTP to retrieve 57
- data.txt file, importing into spreadsheet 57
- Date & Time settings 105, 106
- Delete SSH Host Keys and SSL Certificates 107
- Device IP Configuration Wizard
 - using to configure required TCP/IP settings 150
- Device Manager menu
 - control console 22
- DHCP
 - After IP Assignment setting 112
 - APC cookie 114
 - Boot mode settings 74
 - Communication
 - Vendor Class 75
 - communication settings 75
 - Cookie Is setting 112, 113
 - DHCP & BOOTP boot process 111
 - DHCP Only boot mode setting 74
 - Remain in DHCP & BOOTP mode setting 112
 - Require vendor specific cookie to accept DHCP Address setting 112, 113
 - response options 114
 - Retry Then Stop setting 113
 - Status LED indicating DHCP requests 13

- DHCP & BOOTP boot mode setting 74
- Disabling
 - e-mail to a recipient 67
 - event logging 61
 - Reverse DNS Lookup 77
 - sending any traps to an NMS 63
 - sending authentication traps to an NMS 63
 - Syslog 86

- Domain Name setting 74, 112
- Domain names
 - for trap receivers 63
 - overriding expansion of host name to domain name 75

E

- E-mail
 - configuring 64
 - enabled by default for severe events 62
 - enabling and disabling 67
 - Events menu option 62
 - message format (long or short) 67
 - setting up an account 67
 - using for paging 66
- Email recipients 66
 - format 67
- Enabling
 - e-mail forwarding to external SMTP servers 67
 - e-mail to a recipient 67
 - Reverse DNS Lookup 77
 - sending any traps to an NMS 63
 - sending authentication traps to an NMS 63
 - SSH 80
 - Syslog 86
 - Telnet 80
- Encryption
 - with SSH and SCP 122

- with SSL 88
- Error messages
 - for firmware file transfer 170
 - from overridden values during .ini file transfer 159
- Ethernet Port Speed setting 112
- Event Log
 - accessing 21
 - disabling 61
 - errors from overridden values during .ini file transfer 159
 - using FTP del command 59
 - using FTP to retrieve 57
- event.txt file
 - contents 57
 - importing into spreadsheet 57
- Events menu
 - Actions 60
 - E-mail (Web interface) 62
 - Event Log 61
 - SNMP traps 62

F

- Facility setting 86
- File Transfer 107
- Fingerprints, displaying and comparing 79
- Firewall, as essential to security 133
- Firmware
 - benefits of upgrading 162
 - file transfer methods 165
 - FTP or SCP 166
 - XMODEM 168
 - files for Network Management Card 162
 - obtaining the latest version 163
 - upgrading 162
 - verifying upgrades and updates 170
- Firmware versions displayed on main screen 19

- Follower outlet groups 33
- From Address 65
- FTP 77
 - disabling when SCP is used 78
 - to retrieve text version of Event or Data log 57

G

- Generation (e-mail recipients) 67
- Global outlet groups 33
 - creating 38
 - verifying setup and configuration 41
- Global outlets 33

H

- Help
 - About System option (Web interface) 31
 - on control console 21
- Host keys
 - creating 146
 - file name 83
 - file status 83
 - fingerprints
 - displaying for versions 1 and 2 84
 - generated by the PDU 79
 - transferring to the PDU 79, 83
- Host Name setting 74, 112
- HTTP Port 91
- HTTP protocol mode 90
- HTTPS Port 91
- HTTPS protocol mode 90
- Hyperlinks, defining 108

I

- Identification fields on main screen 19
- InfraStruXure Manager 1

ini files, See User configuration files
Initiator outlet groups 33
IP addresses
 of DNS server for e-mail 64
 of trap receivers 63
 to limit access to specified NMSs 85

K

keywords
 user configuration file 154

L

Life support policy 173
Link (as an outlet setting) 44
Links
 redirecting user-definable links 32,
 108
Local outlet groups 33
 creating 37
Local SMTP server 67
Lock icon indicating SSL is enabled. 90
Logging on
 control console 15
 Web interface 24
Login date and time
 control console 19
 Web interface 27

M

Main screen
 displaying identification 19
 firmware values displayed 19
 login date and time 19
 status 20
 Up Time 19
 User access identification 19

Manual boot mode setting 74

Menus

Control Console 22
Data 30, 69
event-related 30
Events 30
Help 31
Links 108
Network 31
System 31
Web interface 29

N

Network menu

DNS 76
Email 85
FTP Server 77
ISX Protocol 95
Ping utility 77
SNMP 84
Syslog 86
TCP/IP 73
Telnet/SSH 78
WAP 95
Web/SSL 88

NMS IP setting/Domain
 Name Setting 85

O

On Retry Failure setting 76
OS, APC 31
Outlet events
 described 43
Outlet groups
 creating local groups 37
 deleting 38
 editing 38

- enabling 37
 - follower 33
 - global 33
 - initiator 33
 - local 33
 - purpose and benefits 34
 - rules for configuring 36
 - system requirements 35
 - typical configurations 39
- Outlet Name 44
- Outlet settings
- configuring 44
 - controlling outlets 42
- Outlets
- global 33
- Override keyword, in user configuration file 154

P

- Paging by using e-mail 66
- Password change for security 119
- Passwords
- default for each type of account 24
 - for NMS that is a trap receiver 63
 - User Manager access 98
 - using non-standards ports as extra passwords 120
- PDU, port assignment 120
- Port Speed setting 75
- Ports
- assigning 120
 - default
 - for FTP Server 78
 - for HTTP 91
 - for HTTPS 91
 - for SSH 81
 - for Telnet 81
 - using a non-default port
 - for FTP 78
 - for HTTP 91

- for HTTPS 91
 - for SSH 81
 - for Telnet 81
- Power Off Delay 44
- Power On Delay 44
- Primary NTP Server 106
- Primary Server Secret setting for RADIUS 102
- Primary Server setting for RADIUS 102
- Protocol Mode
- selecting for control console access 80
 - selecting for Web access 90

R

- RADIUS settings 101
- Configuring the Rack PDU 102
 - Configuring the RADIUS server 103
- Read access by an NMS 85
- Reboot 107
- outlets 43
 - preventing automated reboot for inactivity 14
- Reboot Duration 44
- Receiver NMS IP/Domain Name 63
- Recipient's SMTP server 67
- Reset
- Only TCP/IP to Defaults 107
 - to Defaults 107
 - to Defaults Except TCP/IP 107
- Retry Then Fail setting 75
- Retry Then Stop setting (DHCP) 113
- Reverse DNS Lookup 77
- Root certificates, creating 137

S

- Scheduling outlet events 49
- SCP
- enabled and configured with SSH 78,

- 123
- Secondary NTP Server 106
- Secondary Server for RADIUS 102
- Secondary Server Secret for RADIUS 102
- Section headings, user configuration file 154
- Secure CoPy. *See* SCP.
- Secure Hash Algorithm (SHA) 92
- Secure SHell. *See* SSH.
- Secure Sockets Layer. *See* SSL.
- Security
 - authentication
 - authentication vs. encryption 120
 - through digital certificates with SSL 124
 - certificate-signing requests 125
 - disabling less secure interfaces 123
 - encryption with SSH and SCP 122
 - how certificates are used 134
 - How SSH host keys are used 135
 - immediately changing username and password 119
 - options for each interface 117
 - planning and implementing 117, 120
 - SCP as alternative to FTP 123
 - SSL
 - choosing a method to use certificates 126
 - CipherSuite algorithms and ciphers 125
 - supported SSH clients 79
 - using non-standards ports as extra passwords 120
- Security Wizard 134
 - creating certificates
 - without a Certificate Authority 137
 - creating server certificates
 - to use with a Certificate Authority 142
 - creating signing requests 142
 - creating SSH host keys 146
- Send DNS Query 76
- Server certificates
 - creating to use with a Certificate Authority 142
 - creating without a Certificate Authority 137
- Severity levels of events 61
 - events with no severity level 61
 - mapping event severity to Syslog priorities. 87
- Signing requests
 - creating 142
- SMTP
 - From Address 65
 - Server 65
 - server 67
 - SMTP Server 65
- SNMP
 - Access Type setting 85
 - Authentication Traps 63
 - Community Name setting 84
 - NMS IP/Domain Name setting 85
 - SNMP traps option 62
- SSH
 - enabling 78
 - encryption 122
 - fingerprints, displaying and comparing 79
 - host key
 - as identifier that cannot be falsified 122
 - creating 146
 - file name 83
 - file status 83
 - transferring to the PDU 79
 - modifying the Port setting 81, 91
 - obtaining an SSH client 79
 - server configuration 82
 - v1 Encryption Algorithms 82
 - v2 Encryption Algorithms 82
- SSL

- authentication through digital certificates 124
 - certificate signing requests 125
 - encryption ciphers and hash algorithms 92
- Status
 - in Web interface 27
 - on control console main screen 20
- Syslog
 - defining Server IP addresses/domain names 87
 - enabling and disabling 86
 - Facility setting 86
 - message format 88
 - sending a test message 87
 - setting the UDP port 87
 - Syslog setting 86
- System information, obtaining 31
- System menu
 - About System (in control console) 108
 - Date & Time 105
 - Identification 105
 - Links 108
 - Modem (not supported) 108
 - Outlet User Manager 99
 - RADIUS 101
 - settings 102
 - Tools 107
 - User Manager 98
- System requirements, outlet groups 35
- T**
- TCP/IP
 - Boot mode 74
 - Client ID setting 75, 112
 - default gateway 73, 74
 - defining settings 73
 - Domain Name setting 74, 112
 - Ethernet Port Speed setting 112
 - Host Name setting 74, 112
 - On Retry Failure setting 76
 - Port Speed setting 75
 - Retry Then Fail setting 75
 - setting port assignments for extra security 120
 - subnet mask 73, 74
 - system IP address 73, 74
 - User Class setting 75, 112
 - Vendor Class setting 75, 112
- Telnet/SSH
 - Access option 80
 - host key fingerprints displaying 84
 - modifying the Port settings 81
 - option in Network menu 78
 - selecting the protocol mode 80
 - SSH host key file name 83
 - SSH host key file status 83
 - SSH Port option 81
 - SShv1 Encryption Algorithms 82
 - SShv2 Encryption Algorithms 82
 - Telnet Port option 81
- Testing the network connection to the DNS server 76
- Time Zone 106
- Timeout setting for RADIUS 102
- To address 66
- Tools menu 107
 - Delete SSH Host Keys and SSL Certificates 107
 - File Transfer 107
 - Reboot 107
 - Reset Only TCP/IP to Defaults 107
 - Reset to Defaults 107
 - Reset to Defaults Except TCP/IP 107
 - Upload (a user configuration file) 107
- Transport Layer Security (TLS) 124
- Trap Generation 63
- Trap Receivers 63
- Traps 63

U

Up Time

- control console main screen 19
- Web interface 27

Update Interval 106

Upgrading firmware

- without using a utility 162

Upload a user configuration file 107

URL address formats 26

User access identification, control console interface 19

User Class setting 75, 112

User configuration files

- contents 154
- customizing 156
- exporting system time separately 156
- overriding device-specific values 154
- retrieving and exporting 153
- system event and error messages 158
- using the APC utility to retrieve and transfer the files 155, 168

User Manager, defining access values and authentication 98

User Name

- change immediately for security 119
- default for each type of account 24
- User Manager access 98

V

Vendor Class setting 75, 112

Vendor Specific Information

- Cookies 114

W

WAP 95

Web interface

- enable or disable protocols 90

logging on 24

Modifying the Port setting

- for FTP 78
- for HTTP 91
- for HTTPS 91
- for SSH 81
- for Telnet 81

Status 27

Up Time 27

URL address formats 26

Wireless Access Protocol (WAP) 95

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
 - www.apc.com (Corporate Headquarters)
Connect to localized APC Web sites for specific countries, each of which provides customer support information.
 - www.apc.com/support/
Global support searching APC Knowledge Base and using e-support.
- Contact an APC Customer Support center by telephone or e-mail.
 - Regional centers:

| | |
|--|--------------------------------|
| Direct InfraStruXure Customer Support Line | (1)(877)537-0607 (toll free) |
| APC headquarters U.S., Canada | (1)(800)800-4272 (toll free) |
| Latin America | (1)(401)789-5735 (USA) |
| Europe, Middle East, Africa | (353)(91)702000 (Ireland) |
| Japan | (0) 35434-2021 |
| Australia, New Zealand, South Pacific area | (61) (2) 9955 9366 (Australia) |

- Local, country-specific centers: go to www.apc.com/support/contact for contact information.

Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

Copyright

Entire contents © 2005 American Power Conversion. All rights reserved. Reproduction in whole or in part without permission is prohibited. APC, the APC logo, InfraStruXure, and PowerNet are trademarks of American Power Conversion Corporation and may be registered in some jurisdictions. All other trademarks, product names, and corporate names are the property of their respective owners and are used for informational purposes only.

990-1368D-001

04/2005

